

Cyber Risk GmbH  
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341  
Dammstrasse 16, 8810 Horgen, Switzerland  
Tel: +41 79 505 89 60 Web: <https://www.cyber-risk-gmbh.com>



*February 2023, top cyber risk and compliance related  
local news stories and world events*

Dear readers,

Can you believe that one day you will read a directive, and you will learn that if a deadline in cybersecurity is missed, the CEO (for EU firms) or the legal representative (for non-EU firms) will be *prohibited* temporarily from exercising managerial functions? No, this is not a joke, this is *Article 32 of the new NIS 2 Directive* of the EU.



According to Article 32, Member States shall ensure that their competent authorities have the power to establish a *deadline* by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities.

If the requested action is *not taken within the deadline* set, Member States shall ensure that their competent authorities have the power to:

(a) suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;

(b) request that the relevant bodies, courts or tribunals, in accordance with national law, **prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level** in the essential entity from **exercising managerial functions** in that entity.

5. Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, Member States shall ensure that their competent authorities have the power to **establish a deadline** by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities. If the **requested action is not taken within the deadline set**, Member States shall ensure that their competent authorities have the power to:

- (a) suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity;
- (b) request that the relevant bodies, courts or tribunals, in accordance with national law, **prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions** in that entity.

The European Union knows how to make cybersecurity important for the CEO. According to Article 20 of NIS 2 (Governance), the management bodies of essential and important entities must approve the cybersecurity risk-management measures taken by those entities, oversee its implementation, and can be held **liable for infringements**.

According to Article 21 (Cybersecurity risk-management measures), essential and important entities must take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

The measures shall be based on an **"all-hazards approach"** that aims to protect network and information systems and the physical environment of those systems from incidents.

**Important note for Non-EU entities:** Under Article 26 (Jurisdiction and territoriality), if an entity is not established in the EU, but offers services within the EU, it shall designate a representative in the EU.

The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established.

In the absence of a representative, **any Member State** in which the entity provides services **may take legal actions against the entity** for the infringement of this Directive.

The war in Europe has some interesting consequences for cybersecurity. I will not be surprised if the European Union institutions complain, at some point in the

future, that the USA needs to be more serious in fighting cyber crime and protecting the critical infrastructure. 😊

Read more at number 1 below.

---

It is February 2023, one year after a major development.

February 2022 was an important month for *hydrogen* production, distribution, storage, use, research and development.

After the outbreak of the war in Ukraine, the European Union decided to phase out Russian energy imports as quickly as possible. The political commitments and decisions to replace fossil fuels were well accepted by all advocates of a clean energy future that ask for the decarbonization of many major industries. Hydrogen plays a key role in this clean energy future.

Technologies for the production, storage, transportation and use of hydrogen as an energy source are available today, but investments are necessary for the broader application that requires scaling up solutions.

Hydrogen may be produced through a variety of processes. Some are clean, some are not so clean:

1. *'Electricity-based hydrogen'* refers to hydrogen produced through the electrolysis of water (in an electrolyser, powered by electricity), regardless of the electricity source. The full life-cycle greenhouse gas emissions of the production of electricity-based hydrogen depends on how the electricity is produced.
2. *'Renewable hydrogen' or 'Clean hydrogen'* is hydrogen produced through the electrolysis of water (in an electrolyser, powered by electricity), and with the electricity stemming from renewable sources. The full life-cycle greenhouse gas emissions of the production of renewable hydrogen are close to zero. Renewable hydrogen may also be produced through the reforming of biogas (instead of natural gas) or biochemical conversion of biomass, if in compliance with sustainability requirements.
3. *'Fossil-based hydrogen'* refers to hydrogen produced through a variety of processes using fossil fuels as feedstock, mainly the reforming of natural gas or the gasification of coal. This represents the bulk of hydrogen produced today. The life-cycle greenhouse gas emissions of the production of fossil-based hydrogen are high.
4. *'Fossil-based hydrogen with carbon capture'* is a subpart of fossil-based hydrogen, but where greenhouse gases emitted as part of the hydrogen production process are captured. The greenhouse gas emissions of the production of fossil-based hydrogen with carbon capture or pyrolysis are lower than for fossil-fuel based hydrogen, but the variable effectiveness of greenhouse gas capture (maximum 90%) needs to be taken into account.

The 8th of July 2020, the European Commission released the communication with title "A hydrogen strategy for a climate-neutral Europe". According to the Commission, hydrogen is enjoying a *renewed and rapidly growing attention* in Europe and around the world.

Hydrogen can be used as a feedstock, a fuel or an energy carrier and storage, and has many possible applications across industry, transport, power and buildings sectors. Most importantly, it does not emit CO<sub>2</sub> and almost no air pollution when used. It thus offers a solution to decarbonise industrial processes and economic sectors where reducing carbon emissions is both urgent and hard to achieve.

All this makes hydrogen essential to support the EU's commitment to reach carbon neutrality by 2050 and for the global effort to implement the Paris Agreement while working towards zero pollution. Technological developments and the urgency to drastically reduce greenhouse emissions, are opening up new possibilities. Every week new investment plans are announced, often at a gigawatt scale.

Between November 2019 and March 2020, market analysts increased the list of planned global investments from 3,2 GW to 8,2 GW of electrolyzers by 2030 (of which 57% in Europe) and the number of companies joining the International Hydrogen Council has grown from 13 in 2017 to 81.

**In transport**, hydrogen is also a promising option where electrification is more difficult. In a first phase, early adoption of a hydrogen can occur in captive uses, such as local city buses, commercial fleets (e.g. taxis) or specific parts of the rail network, where electrification is not feasible. Hydrogen refuelling stations can easily be supplied by regional or local electrolyzers, but their deployment will need to build on clear analysis of fleet demand and different requirements for light- and heavy-duty vehicles.

Hydrogen fuel cells should be further encouraged in **heavy-duty road vehicles**, alongside electrification, including coaches, special purpose vehicles, and long-haul road freight given their high CO<sub>2</sub> emissions. The 2025 and 2030 targets set out in the CO<sub>2</sub> Emission Standards Regulation are an important driver to create a lead market for hydrogen solutions, once fuel cell technology is sufficiently mature and cost-effective. Projects of the Horizon 2020 Fuel Cells and Hydrogen Joint Undertaking (FCH-JU) are aiming to accelerate Europe's technological lead.

**Hydrogen fuel-cell trains** could be developed to more viable train commercial routes that are difficult or not cost-effective to electrify: about 46 % of the mainline network is still being served by diesel technology today. Certain fuel-cell hydrogen train applications (e.g. Multiple Units) can already be cost competitive with diesel today.

For **inland waterways and short-sea shipping**, hydrogen can become an alternative low emission fuel, especially since the Green Deal emphasises that CO<sub>2</sub> emission in the maritime sector must have a price. Scaling up fuel cell power from one<sup>42</sup> to multiple megawatts and using renewable hydrogen for the

production of synthetic fuels, methanol or ammonia - with higher energy density – are required for longer-distance and deep-sea shipping.

Hydrogen can become in the longer-term an option to decarbonise the **aviation and maritime sector**, through the production of liquid synthetic kerosene or other synthetic fuels. These are “drop-in” fuels that can be used with existing aircraft technology, but implications in terms of energy efficiency have to be taken into account.

In the longer-term, hydrogen-powered fuel cells, requiring adapted aircraft design, or hydrogen-based jet engines may also constitute an option for aviation. To realise these ambitions will require a roadmap for the considerable long-term research and innovation efforts, including under Horizon Europe, the Fuel Cell and Hydrogen Joint Undertaking and possible initiatives as part of the Hydrogen Alliance.

---

To the extent that international trade is negatively affected by geopolitical factors, a trend towards *regionalisation* will emerge, as a mechanism to continue to enjoy the benefits of globalisation but on a smaller scale. As an illustration, in 2022, 44% of global companies were developing regionalised supply networks (up from only 25% in 2021).

This is part from an excellent presentation from Pablo Hernández de Cos, Governor of the Bank of Spain, at the Dialogue with the Governor on the Future of Globalisation, Cañada Blanch Centre for Contemporary Spanish Studies and London School of Economics and Political Science, in London.

Pablo Hernández de Cos explained that in response to these challenges, the EU has recently been launching a series of policies within the so-called *Open Strategic Autonomy agenda* - an emerging set of regulatory, structural and fiscal policies that seek to address the EU's economic vulnerabilities arising from geopolitical considerations. Under the framework of Open Strategic Autonomy, *three* types of policies have been proposed to reduce the EU's vulnerabilities.

A *first* set of measures aims to assess supply chain dependencies and vulnerabilities and *increase the resilience of the European industrial system*.

Specific examples are the action plan on critical raw materials - aimed at reducing the EU's external dependence in the sourcing of such goods -, the "RePowerEU" initiative - aimed at reducing the EU's energy dependence -, and plans to drive the digitalisation of European economies.

A *second* set of measures aims to protect EU countries from possible abusive practices adopted by third economies - practices that may be related to strategic or political objectives.

These measures include those aimed at monitoring foreign direct investment flows from third countries and other measures designed to limit coercive actions against European companies.

A *third* class of measures aims to preserve the international level playing field by compensating for competitive disadvantages that EU companies might face due to less stringent environmental and state aid policies implemented by third countries.

Examples are the regulation on foreign subsidies that distort the internal market and the Carbon Border Adjustment Mechanism (CBAM).

Pablo Hernández de Cos also explained that it is essential to make progress in **extending risk-sharing mechanisms** – public and private - in the EU. This should be done in *three* ways.

*First*, the Economic and Monetary Union (EMU) needs to equip itself with a permanent macroeconomic stabilisation capacity.

*Second*, it is essential that the Banking Union be completed with the construction of an EU deposit guarantee system.

And *third*, progress in building the Capital Markets Union is essential to increase the resilience of the EMU to macro-financial shocks, better spread the costs of asymmetric or idiosyncratic shocks, reduce the risks of financial fragmentation, and provide a more favourable environment for private investment.

According to Pablo Hernández de Cos, for the time being there is no consistent trend towards “deglobalisation”, but rather a change in the nature of globalisation, leading to a rise in the regionalisation of trade and supply chains, a diversification of sourcing and a certain slowdown in global value chain fragmentation.

While the marked slowdown in firms’ decisions to relocate part of their production processes abroad (“offshoring”) or to repatriate previously offshored activities (“reshoring”) is compatible with a deglobalisation phase, other factors qualify this view.

The flattening of trade in goods does indeed hint at a trend slowdown, but the continued growth of international trade in services seems to signal a continuation of globalisation trends in these sectors, driven by technological progress, including data trading and the expansion of *artificial intelligence*.

Read more at number 10 below.

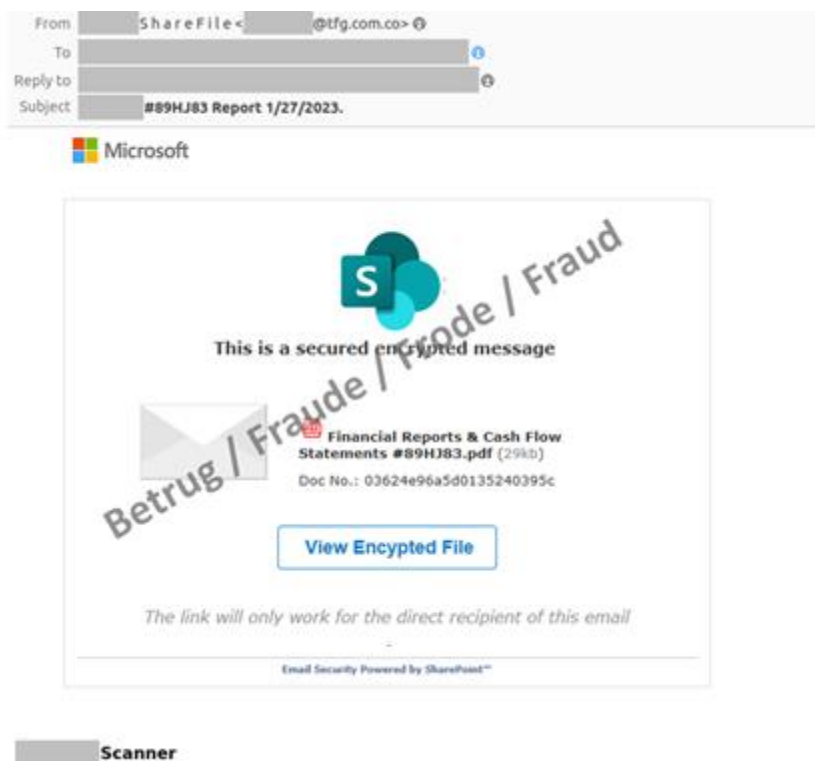
---

In Switzerland, according to the National Cyber Security Centre (NCSC), we have attacks on Microsoft Office 365 accounts. These accounts are often secured with a *second factor* and are therefore harder to hack. So attackers are going to considerable lengths, using *real-time phishing* to obtain login credentials. They use the stolen credentials to send phishing emails or for business email compromise attacks.

Virtually all Microsoft Office 365 access is now secured with a second factor. In addition to the email address and a password, a second factor – a code sent by text message or a token generated by an app – is required. However, the second factor is only valid for a limited period. So in order to steal the login credentials, the attackers have to act within a certain time.

A current example, which was reported to the NCSC last week, is described in more detail below.

According to the National Cyber Security Centre, the attack began with an email which was disguised as a scanned document from a photocopier and claimed to contain a financial report in the form of an encrypted file.



The phishing email claims to be from a scanner and to contain an encrypted financial report. The link leads, via a few detours, to the phishing site.

The attackers cannot be certain when the email was opened, or the phishing link clicked on. So in order to gain time and avoid having to react immediately when the victim clicks on the phishing link, the phishers first **demand proof that there is a human behind the request**. This enables them to prolong the login procedure slightly.

The apparent "verification page", aimed at gaining time for the request. The site is hosted in Russia and requires several mouse clicks. After the "verification" is successful, the victim is automatically forwarded to the phishing site.

As soon as the victim clicks on the link, a phishing page bearing the logo of the company – or this case the commune – is generated dynamically and the victim's

email address is displayed. After a correct user name and password are entered, the second factor is requested. For this purpose, the attackers log on in the background and trigger the text message or authentication token. They then load another page where this second factor can be entered.

The phishing page looks innocuous and displays the commune's logo. The victim's email address is pre-filled. After the correct user name is entered, the second factor is requested.

If someone enters their login credentials on the phishing site, the second factor needs to be processed as soon as possible and automatically, so that the Office365 access thus obtained can be used.

Because of the second factor, this attack method is known as **real-time phishing**. The attackers cannot collect details for later use. They have to act immediately – i.e. in real time.

Having intercepted the second factor, the attackers can now log into the hacked account themselves and use it either in an automated process or "by hand". In this case, automation helps the attackers. For example, when automatic email forwarding is set up, emails are often sent to all contacts in the phone book. This increases the likelihood that other people will take the bait.

Things get really interesting when the hacked Office 365 account **contains emails with payment information or invoices**. The attackers can use them to perform a so-called **business email compromise (BEC)** and change the account information in the invoices. So rather than the victim paying the invoice amount to the legitimate recipient, the money goes to a fraudulent account.

It is also easier to send software, since the recipients know and trust the hacked sender.

Luckily, the phishing attempt reported to the NCSC was not successful, owing to the perspicacity of the recipient.

#### *Recommendations from the NCSC:*

- Never enter a password or credit card number on a page you reached via a link in a message. It is most likely a phishing attempt;
- Check any website requesting your login credentials very carefully. Two-factor authentication does not protect you from real-time phishing.

---

The human element in cybersecurity is the weakest link. In Switzerland, according to the National Cyber Security Centre (NCSC), we have also telephone phishing attacks. The NCSC describes the modus operandi very well:



## Telephone phishing: A drama in four acts

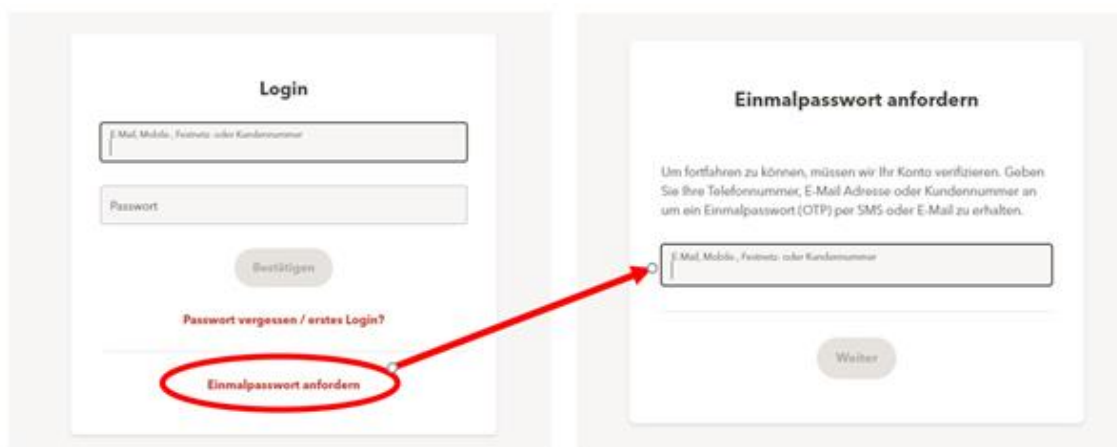
Phishers are thinking up all sorts of new tricks to persuade their victims to hand over access to the payment functions of their phone and their credit card details. A new and very sophisticated method was reported to the NCSC last week.

### Act I: Establish trust and obtain information

The fraud begins with a WhatsApp call from someone claiming to be from a telecoms provider. The caller claims that the reason for phoning via WhatsApp is because the phone number is currently blocked owing to the activation of the 6G network, and offers to guide the victim through the unblocking process. The victim is promised compensation of CHF 400 for the blockage.

During the phone call, the attacker enters the victim's phone number on the telecoms provider's official portal, which causes a one-time code to be issued. The bogus employee now asks the victim to read aloud the code, which has now arrived by text message. The code allows the attackers to log into the telecom provider's portal without needing any further details, and to look at the client documentation, including the contract.

The attackers exploit the fact that, in addition to the login method involving the user name and password, it is also possible to log in using only a one-time code sent to the person's phone. This means that the user name and password are not necessary.



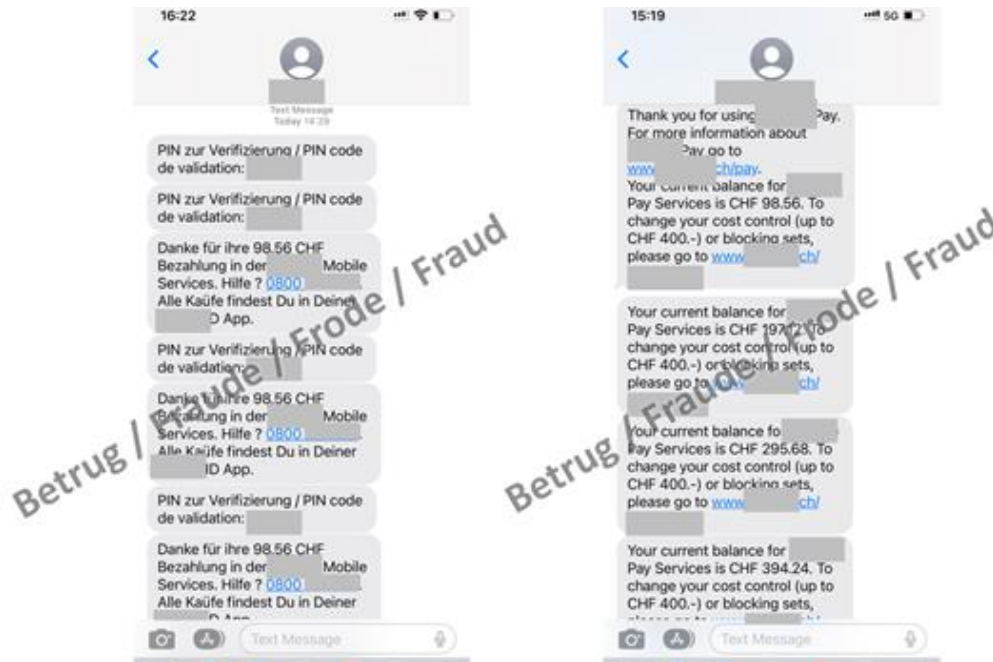
During login, the user name and password are requested (left-hand image). But it is also possible to perform authentication using just a code sent to the registered phone number (right-hand image). Once the attackers know the one-time password, they can log in without needing any other details.

During login, the user name and password are requested (left-hand image). But it is also possible to perform authentication using just a code sent to the registered phone number (right-hand image). Once the attackers know the one-time password, they can log in without needing any other details.

## Act II: Using the payment service

Now that they have access to the client account, the attackers can activate the phone's payment function. This function is used to make purchases from partner companies and pay for them via the phone bill. However, this function also needs to be activated using a one-time code. The limit for such purchases is CHF 400. In order not to exceed this limit, the attackers now make four purchases for EUR 100 each – probably gift vouchers as they are practically untraceable – from one of the registered businesses.

Here too, the attackers manage to persuade the victims to read the codes aloud. They claim that the amounts displayed will be credited to the victim.



The first PIN gives access to the client portal, while the others are probably used to purchase gift vouchers. Each deducted amount is EUR 100. The victims are tricked into thinking that the amounts will be credited to their account.

The first PIN gives access to the client portal, while the others are probably used to purchase gift vouchers. Each deducted amount is EUR 100. The victims are tricked into thinking that the amounts will be credited to their account.

## Act III: Credit card phishing

Yet the attackers are not satisfied with only gift vouchers. Now they try and phish for credit card details. So someone else calls via WhatsApp, and also claims to be from customer services.

To prove that they are genuine, they send the client contract which they obtained in Act I.



The adviser, called "Setephen", makes contact from a number in Pakistan. The original contract displayed comes from the client portal. Below that is the link to the phishing site.

The adviser, called "Setephen", makes contact from a number in Pakistan. The original contract displayed comes from the client portal. Below that is the link to the phishing site.

The message recipient is now supposed to enter their credit card details on a website that purports to be a page of the telecom provider. However, it is a phishing site.



The website with the apparent release of 6G (a standard which does not yet exist). In the right-hand image the entry fields for the credit card details. The explanation for communicating via WhatsApp is in larger font.

The website with the apparent release of 6G (a standard which does not yet exist). In the right-hand image the entry fields for the credit card details. The explanation for communicating via WhatsApp is in larger font.

### Act IV: Happy ending

However, the message recipient thought this was a little too suspicious. They went to one of the telecom provider's shops, where the attack was quickly discovered and stopped. The telecoms provider was generous and did not debit the amount from the payment function. The phishing site was also rapidly blocked after the case was reported.

There is still one fly in the ointment: the private details in the contract fell into the hands of the attackers and could be used for further attacks.

Recommendations from the National Cyber Security Centre:

- Never reveal codes or passwords to people over the phone;
- Set cost limits for payment functions that are as low as possible, or deactivate these functions. The telecoms providers can also permanently block these services;
- If you are unsure, terminate the call and phone back using the provider's official number. You can find the phone number on the official website of the provider concerned;
- Never allow yourself to be put under pressure on the phone;

---

The Swiss National Cyber Security Centre (NCSC) is doing a great job. They describe very well another attack to the human element of cybersecurity, the weakest link.

### False hope for higher minimum pension

The fraud was mainly directed at French citizens. However, last week saw a similar case targeting Swiss citizens.

A website purporting to be run by the AHV claimed that the Federal Council had decided to increase the minimum pension by at least CHF 400.

Here, too, the victim was asked to provide their credit card details in order to receive the promised money.

**Die größte Veränderung in der Rentenreform seit 1997. Die erste Säule hat sich bis zur Unkenntlichkeit verändert**

Durch Steuererhöhungen für große Unternehmen sowie durch das Wachstum der Wirtschaft des Landes. Der 7-köpfige Bundesrat hat einstimmig beschlossen, die Mindestrente um 400 Franken zu erhöhen. Und sie ordneten an, diese Erhöhung sofort zu bezahlen, nachdem sie Ihre Identität mit einer Bankkarte bestätigt hatten.



**Geben Sie Ihre Kreditkartendaten ein und erhalten Sie jetzt eine gesetzliche Rentenerhöhung!**

Kreditkartennummer  
XXXX XXXX XXXX XXXX

Gültigkeitsdatum 01/23 CVV/CVC Code 999

Name des Karteninhabers  
Il tuo nome e cogn

**400 Fr bekommen**



Using a purported statement by National Councillor Martullo-Blocher and a document allegedly signed by all the Federal Councillors, the fraudsters tried to gain the victim's trust. Here, too, the attackers tried to obtain credit card information. The NCSC was able to take down the website.

Der Bundesrat hat die Renten von AHV und IV gemäss dem im AHV-Gesetz vorgeschriebenen Massstab angepasst. Die Renten müssen alle zwei Jahre geprüft werden, so sie an die Teuerung und die Entwicklung der Löhne angepasst werden müssen. Dabei wird die Empfehlung der Eidgenössischen AHV/IV-Kommission berücksichtigt. Dieses Mal werden 400 Franken zu jeder Rente hinzugefügt. Die Erhöhung berücksichtigt bei der letzten Abstimmung die Wünsche des Volkes. Rentner sollen sich nicht benachteiligt fühlen.

*(Faked signatures of federal councilors)*

**Magdalena Martullo-Blocher**

SVP-Nationalrätin und Schweizer Unternehmerin

Das System der staatlichen Rentenversicherung wurde 1948 im Land eingeführt, und seitdem wurden zehn Reformen durchgeführt, die wahrscheinlich die wichtigste soziale Eroberungsmacht der letzten hundert Jahre in der Schweiz darstellen. Das letzte Mal ist es 1987 passiert.

Darüber hinaus gibt es für die Bevölkerung keine Möglichkeit, Steuern zu senken, die Renten kürzungen vorzuziehen. Solche Projekte wurden bereits dreimal in Referenden abgelehnt. Es gibt jetzt keine Möglichkeit, Steuern zu erhöhen. Das einfache Volk ist zu solchen Maßnahmen nicht bereit.

Aber große Unternehmen und Unternehmen sind dazu bereit. Durch die Renten den Lebensstandard nach der Pensionierung...



**Recommendations from the National Cyber Security Centre (NCSC):**

- Never divulge personal data such as passwords or credit card details on a website that you accessed by clicking on a link in an email or text message.

- Bear in mind that email sender IDs can easily be spoofed.
- Be sceptical if you receive emails that require action on your part and that carry a threat of consequences (loss of money, criminal charges or criminal proceedings, blocking of an account or card, missed chance, misfortune) if you do not do what is required.
- Be particularly sceptical of emails that put you under time pressure.

Welcome to our monthly newsletter.

Best regards,

*George Lekatis*

George Lekatis  
General Manager, Cyber Risk GmbH

Visit our reading room at:

[https://www.cyber-risk-gmbh.com/Reading\\_Room.html](https://www.cyber-risk-gmbh.com/Reading_Room.html)



[ABOUT](#) [TRAINING](#) [FOR THE BOARD](#) [ASSESSMENT](#) [READING ROOM](#) [CONTACT](#) [CYBER RISK LINKS](#) [IMPRESSUM](#)

1. Article for Heise's IX Magazine (in German): "Sicherheitsrisiko Mitarbeiter: Mit Psychologie Cybersecurity-Kultur Schärfen Der Mensch ist das schwächste Glied in der IT-Security-Kette. Psychologisches Know-how hilft beim Aufbau einer Cybersecurity-Kultur."

<https://www.heise.de/hintergrund/Sicherheitsrisiko-Mitarbeiter-Mit-Psychologie-Cybersecurity-Kultur-schaerfen-7187096.html>

heise +

## Sicherheitsrisiko Mitarbeiter: Mit Psychologie Cybersecurity-Kultur schärfen

Der Mensch ist das schwächste Glied in der IT-Security-Kette. Psychologisches Know-how hilft beim Aufbau einer Cybersecurity-Kultur.

Leszeit: 22 Min. In Pocket speichern

1



*Number 1 (Page 19)*

The NIS 2 Directive of the EU



*Number 2 (Page 22)*

Think before you link

**CPNI**

Centre for the Protection  
of National Infrastructure

*Number 3 (Page 24)*

Phishing Resistance – Protecting the Keys to Your Kingdom



*Number 4 (Page 28)*

Measuring The Effectiveness of Celebrity Activism: Celebrity Advocate v Celebrity Endorser

Donara Barojan, MA in Strategic Communications from King's College London



*Number 5 (Page 29)*

Statement by National Security Advisor Jake Sullivan on the New U.S.-EU Artificial Intelligence Collaboration

**THE  WHITE HOUSE**

*Number 6 (Page 31)*

Engineering Personal Data Sharing



*Number 7 (Page 35)*

Countering Human Trafficking Year in Review

U.S. Department of Homeland Security (DHS)



Homeland  
Security



Center for Countering  
Human Trafficking

*Number 8 (Page 37)*

## ECONOMIC AND NATIONAL SECURITY IMPLICATIONS OF THE COVID-19 PANDEMIC THROUGH 2026

Office of the  
Director of National Intelligence

*Number 9 (Page 40)*

## How Cybersecurity Standards Support the Evolving EU Legislative Landscape



*Number 10 (Page 42)*

## (De)globalisation and economic policies in the European context

Pablo Hernández de Cos, Governor of the Bank of Spain, at the Dialogue with the Governor on the Future of Globalisation, Cañada Blanch Centre for Contemporary Spanish Studies and London School of Economics and Political Science, London.



*Number 11 (Page 45)*

We had a security incident. Here's what we know.



*Number 12 (Page 47)*

Screen-time: Sometimes It Feels Like Somebody's Watching Me  
**proofpoint.**



*Number 13 (Page 48)*

**Predicting pandemics through museum animal collections**

Coalition studies UNM museum samples to explore pathogens



*Number 14 (Page 50)*

**U.S. Department of Justice Disrupts Hive Ransomware Variant**

FBI Covertly Infiltrated Hive Network, Thwarting Over \$130 Million in Ransom Demands



*Number 15 (Page 53)*

**Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay \$30 Million to Settle SEC Charges**



*Number 16 (Page 55)*

Statement

**Kraken Down: Statement on SEC v. Payward Ventures, Inc., et al.**  
SEC Commissioner Hester M. Peirce



*Number 17 (Page 57)*

**An important next step on our AI journey**

Sundar Pichai, CEO of Google and Alphabet



*Number 18 (Page 59)*

Applying AI to some of the world's biggest challenges



*Number 19 (Page 61)*

The future of AI is now



*Number 20 (Page 64)*

NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices

The algorithms are designed to protect data created and transmitted by the Internet of Things and other small electronics.



## *Number 1*

### The NIS 2 Directive of the EU



Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges.

That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States.

The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems.

As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society.

Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.

Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.

The cybersecurity requirements imposed on entities providing services or carrying out activities which are economically significant vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision.

Those disparities entail additional costs and create difficulties for entities that offer goods or services across borders.

Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities.

Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges.

The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the delimitation of which was very largely left to the discretion of the Member States.

Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards the implementation of the security and incident reporting obligations laid down therein.

Those obligations were therefore implemented in significantly different ways at national level.

There are similar divergences in the implementation of the provisions of Directive (EU) 2016/1148 on supervision and enforcement.

All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures.

Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the Union.

This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations.

Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy to provide a comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market.

In particular, this Directive aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers, which has been proven to be obsolete, since it does not reflect the importance of the sectors or services for the societal and economic activities in the internal market.

To read more: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

27.12.2022

EN

Official Journal of the European Union

L 333/80

**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of 14 December 2022**

**on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)**

**(Text with EEA relevance)**

## *Number 2*

### Think before you link

## CPNI

Centre for the Protection  
of National Infrastructure

Have you ever encountered someone online who was not who they seemed?

In the digital age, online social and professional networking sites are enabling us to be more joined up than ever, but also expose us to unforeseen risks.

Our app can help keep you, your colleagues, and the country safe from being targeted by malicious profiles online.

The Think Before You Link campaign, on which this app is based, is designed to raise awareness of the threat posed by hostile state actors and organised criminals from trying to steal intellectual property or information through social media and professional networking sites.



### *How do they trick you?*

Typically, hostile actors and criminals contact the target posing as an interested 'employer' or recruitment consultant presenting a unique business opportunity.




They ask for further details about the target's background, try to "sell" the business opportunity, and insist on discussing it privately, away from the initial website.

This kind of engagement is an attempt to understand the level of access the individual has to sensitive information, draw it out from them, and build a longer term relationship.

Most of the time the target is not aware of the real purpose of the approach. In some instances, they believe they are providing information to develop a legitimate business opportunity.

### Know the signs

There are many ways in which malicious profiles will try and connect with you. The examples below are just of some of the things to look out for.

<p><b>Too good to be true</b></p> <p>Offering remote, flexible working, a disproportionately high salary for the role advertised.</p>		<p><b>Lack of depth/details</b></p> <p>A lack of any visible or checkable company information available online. The role itself lacks tangible details.</p>		<p><b>Flattery</b></p> <p>Overly focusing on your skills/experience along with a reference to government or 'high end' candidates.</p>	
---	---	---	---	--	---

### *About CPNI*

CPNI is the government authority for protective security advice to the UK national infrastructure. Our role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats. We are accountable to the Director General of MI5.

There are also other nationally important assets or events, including high-profile iconic targets, where impact of damage would be equally serious even though these do not deliver an essential service. Our advice delivery extends to help the protection of such assets and events.

CPNI is committed to equality, diversity and inclusion (EDI). EDI is integral to our culture and working practices, as well as our protective security efforts. We also work closely with key partners to promote greater EDI in the wider security profession.

To read more: <https://thinkbeforeyoulink.app>

## *Number 3*

### Phishing Resistance – Protecting the Keys to Your Kingdom



If you own a computer, watch the news, or spend virtually any time online these days you have probably heard the term “phishing.” Never in a positive context...and possibly because you have been a victim yourself.

Phishing refers to a variety of attacks that are intended to convince you to forfeit sensitive data to an imposter.

These attacks can take a number of different forms; from spear-phishing (which targets a specific individual within an organization), to whaling (which goes one step further and targets senior executives or leaders).

Furthermore, phishing attacks take place over multiple channels or even across channels; from the more traditional email-based attacks to those using voice – vishing – to those coming via text message – smishing.

Regardless of the type or channel, the intent of the attack is the same – to exploit human nature to gain control of sensitive information.

These attacks typically make use of several techniques including impersonated websites, attacker-in-the-middle, and relay or replay to achieve their desired outcome.

Due to their effectiveness and simplicity, phishing attacks have rapidly become the tool of choice for baddies everywhere.

As a tactic, it is used by everyone from low level criminals looking to commit fraud, to the sophisticated nation state attackers seeking a foothold within an enterprise network. And, while almost any kind of information can be targeted, often the most damaging attacks focus on your password, pin, or one-time passcodes – the keys to your digital realm.

The combination can be catastrophic. The Verizon 2022 Data Breach Investigations Report lists phishing and stolen credentials (which may be harvested during phishing attacks) as two of the four “key pathways” that organizations must be prepared to address in order to prevent breaches.

In recognition of the threat posed by phishing – the Office of Management and Budget’s Memo 22-09 “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles” prioritizes implementation of phishing resistant authenticators.



You may visit: <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young  
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

So – how do you keep your keys from falling into the wrong hands? What constitutes a phishing resistant authenticator?

NIST Special Publication DRAFT 800-63-B4 defines it as “the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber.” To achieve this, phishing resistant authenticators must address the following attack vectors associated phishing:

1. **Impersonated Websites** – Phishing resistant authenticators prevent the use of authenticators at illegitimate websites (known as verifiers) through multiple cryptographic measures.

This is achieved through the establishment of authenticated protected channels for communications and methods to restrict the context of an authenticator's use.

For example, this may be achieved through name binding – where an authenticator is only valid for a specific domain (I can only use this for one website). It may also be achieved through binding to a communication channel – such as in client authenticated TLS (I can only use this over a specific connection).

2. **Attacker-in-the Middle** - Phishing resistant authenticators prevent an attacker-in-the-middle from capturing authentication data from the user and relaying it to the relying website.

This is achieved through cryptographic measures, such as leveraging an authenticated protected channel for the exchange of information and digitally signing authentication data and messages.

3. **User Entry** – Phishing resistant authenticators eliminate the need for a user to type or manually input authentication data over the internet.

This is achieved through the use of cryptographic keys for authentication that are unlocked locally through a biometric or pin. No user entered information is exchanged between the relying website and the authenticator itself.

4. **Replay** – Phishing resistant authenticators prevent attackers from using captured authentication data at a later point in time.

Supporting cryptographic controls for restricting context and to prevent attacker-in-the-middle scenarios are also preventative of replay attacks, particularly digitally signed and time-stamped authentication and message data.

As complicated as this may seem, there are several practical examples of phishing resistant authenticators in place today.

For U.S. federal employees, the most ubiquitous form of phishing resistant authenticator is the Personal Identity Verification (PIV) card; they leverage public-key cryptography to protect authentication events.

Commercially, FIDO authenticators paired with W3C's Web Authentication API are the most common form of phishing resistant authenticators widely available today.

These can take the form of separate hardware keys or be embedded directly into platforms (for example your phone or laptop).

Availability, practicality, and security of these “platform authenticators” increasingly puts strong, phishing resistant authenticators into user's hands without the need for additional form factors or dongles.

Not every transaction requires phishing resistant authenticators. However, for applications that protect sensitive information (such as health information or confidential client data) or for users that have elevated privileges (such as admins or security personnel) organizations should be enforcing, or at least offering, phishing resistant authenticators.

Individuals should explore the security settings for their more sensitive online accounts to see if phishing resistant authenticators are available and make use of them if they are. In reality, these tools are often easier, faster, and more convenient than the MFA – such as SMS text codes – they may currently be using.

In the end, phishing resistant authenticators are a critical tool in personal and enterprise security that should be embraced and adopted. They are not, however, a silver bullet.

Phishing resistant authenticators only address one focus of phishing attacks – the compromise and re-use of authenticators such as passwords and one-time passcodes.

They do not mitigate phishing attempts that may have alternative goals such as installing malware or compromising personal information to be used elsewhere.

Phishing resistant authenticators should be paired with a comprehensive phishing prevention program that includes user awareness and training, email protection controls, data loss prevention tools, and network security capabilities.

To read more: <https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom>

*Number 4*

## Measuring The Effectiveness of Celebrity Activism: Celebrity Advocate v Celebrity Endorser

Donara Barojan, MA in Strategic Communications from King's College London



### *Abstract*

The influence of celebrities in politics has long been underestimated in political science and political communications disciplines.

This research explores the effectiveness of two types of celebrity activism—celebrity advocacy and celebrity endorsements—to determine which type produces broader and more focused media coverage.

Through case study analysis, this essay finds that although celebrity advocates and celebrity endorsers generate similarly broad media coverage, celebrity advocates generate media coverage that is more focused on their cause.

In addition, by taking into consideration celebrities' gender, race, and the political leaning of the cause advocated or endorsed by the celebrity, the research finds that all three variables also affect the breadth and the focus of the media coverage, but more quantitative research is required to confirm a causal relationship.

This research has important implications for governmental and non-governmental actors engaging with celebrity endorsers and celebrity advocates—while both are equally capable of generating broad media coverage, celebrity advocates are better suited to retaining the focus of the media coverage on the cause, and not themselves.

To read more: <https://stratcomcoe.org/publications/measuring-the-effectiveness-of-celebrity-activism-celebrity-advocate-v-celebrity-endorser/265>

*Number 5*

## Statement by National Security Advisor Jake Sullivan on the New U.S.-EU Artificial Intelligence Collaboration

### THE WHITE HOUSE

The United States and the European Union signed an administrative arrangement to bring together experts from across the U.S. and Europe to further research on artificial intelligence (AI), computing, and related privacy protecting technologies, as underscored in the U.S.-EU Trade and Technology Council (TTC) commitment.

This collaborative effort will drive responsible advancements in AI to address major global challenges with a joint development model and integrated research to deliver benefits to our societies through five key areas of focus: Extreme Weather and Climate Forecasting, Emergency Response Management, Health and Medicine Improvements, Electric Grid Optimization, and Agriculture Optimization.

Together, we are confident the results of our research will extend beyond our partnership to benefit additional international partners and the global science community.

Today's announcement also builds on the vision set forth in the [Declaration for the Future of the Internet \(DFI\)](#) for an open, free, reliable, and secure Internet and digital technologies around the world.

THE WHITE HOUSE



## FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet

We look forward to deepening our cooperation with the EU through this initiative.

To read more:

<https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/u-s-eu-joint-statement-of-the-trade-and-technology-council/>

[https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet-Launch-Event-Signing-Version\\_FINAL.pdf](https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet-Launch-Event-Signing-Version_FINAL.pdf)

[https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/27/statement-by-national-security-advisor-jake-sullivan-on-the-new-u-s-eu-artificial-intelligence-collaboration/#:~:text=Today%2C%20the%20United%20States%20and,Trade%20and%20Technology%20Council%20\(TTC\)](https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/27/statement-by-national-security-advisor-jake-sullivan-on-the-new-u-s-eu-artificial-intelligence-collaboration/#:~:text=Today%2C%20the%20United%20States%20and,Trade%20and%20Technology%20Council%20(TTC))

## A DECLARATION *for the* FUTURE *of the* INTERNET

*W*e are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is an open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

## Number 6

### Engineering Personal Data Sharing



This report attempts to look closer at specific use cases relating to personal data sharing, primarily in the health sector, and discusses how specific technologies and considerations of implementation can support the meeting of specific data protection.

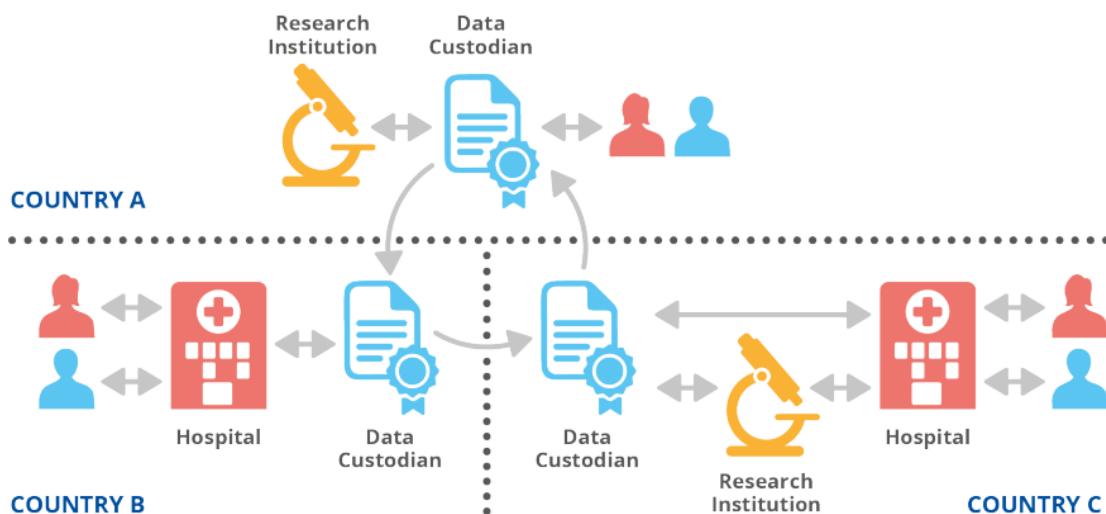
After discussing some challenges in (personal) data sharing, this report demonstrates how to engineer specific technologies and techniques in order to enable privacy preserving data sharing.

More specifically it discusses specific use cases for sharing data in the health sector, with the aim of demonstrating how data protection principles can be met through the proper use of technological solutions relying on advanced cryptographic techniques.

Next it discusses data sharing that takes place as part of another process or service, where the data is processed through some secondary channel or entity before reaching its primary recipient.

Lastly, it identifies challenges, considerations and possible architectural solutions on intervenability aspects (such as the right to erasure and the right to rectification when sharing data).

**Figure 17: Cross border data exchange with data custodians**



When two or more parties decide to share their data, they become part of a larger data ecosystem where they can take advantage of the combined data set that enables the discovery, by way of computation, of new information or trends relating to individuals, groups of individuals, or to society as a whole.

The easiest and most straightforward way to achieve this goal would be to exchange the raw data that each actor holds across technical interfaces putting them on a common table (i.e. a single database) but this hypothetical option is not really feasible.

In reality we are pursuing trusted sharing environments that will make full use of the potential offered by a safe and secure exchange and use of personal data while respecting data protection principles.

This report attempted to look closer at specific use cases relating to personal data sharing, primarily in the health sector, and to discuss how specific technologies and considerations of implementation can support the engineering of personal data sharing in practice.

The analysis ranged from user-controlled data sharing to large scale personal data gathering and data sharing using third party service.

Despite the potential of the data sharing concept and the relevant Union policy and law in the area, there are still considerations on which are the appropriate technical and organizational measures and how to engineer them into practice.

The European legislative initiatives on data sharing described in Section 1.1 entail the processing of large quantities of data which will also include personal data.

Therefore, in addition to the consistency of their provisions with the GDPR, it is important to remove any legal uncertainty on the roles and obligations, not only for individuals as highlighted by the EDPB and the EDPS but also for the entities involved in the data sharing.

In order to leverage the potential of data sharing across the EU, practitioners could be provided with directions on which technologies and techniques can be considered, under which circumstances and which data protection principles can be met.

There are several commonly used (cryptographic) techniques (i.e. asymmetric encryption, pseudonyms, access control etc) that are already acknowledged as able to alleviate data protection risks.



Some of them were discussed in Section 2, Section 3 and Section 4. In emerging concepts such as data spaces and data intermediaries, however, the risks introduced cannot always be adequately addressed only by such techniques.

This is due to the fact that data subjects want to preserve confidentiality of the data they are sharing, they might not know beforehand with whom they might be sharing data with or might want to share accumulated datasets.

Although there are advanced techniques that are still evolving, they should not be considered as of purely academic interest since there exist practical implementations in real use case scenarios.

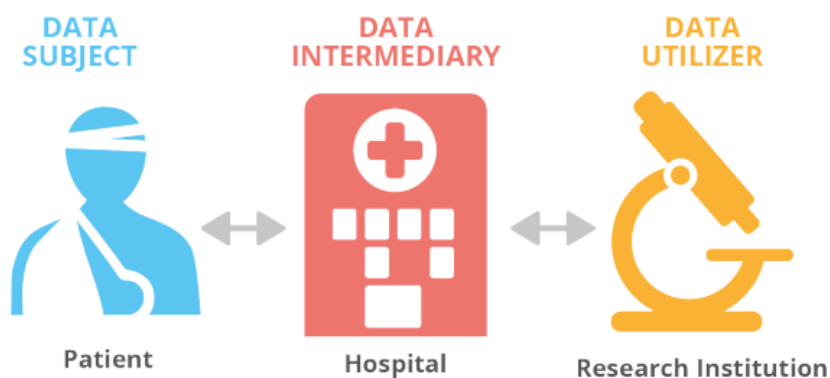
Lastly, since the majority of the technologies described earlier and in previous ENISA reports rely on asymmetric cryptography, the advent of quantum computing and the impact on the security of currently used asymmetric ciphers should be anticipated.

Following the deployment of data sharing infrastructures and services, we cannot expect that they will cease to operate due to possible inadequacy of the asymmetric ciphers.

This is where crypto agility becomes relevant as it allows for a switch between algorithms, cryptographic primitives, and other encryption mechanisms without significant changes in the overall IT system or process.

To read more: <https://www.enisa.europa.eu/publications/engineering-personal-data-sharing>

**Figure 14: Data sharing scenario with data intermediaries**



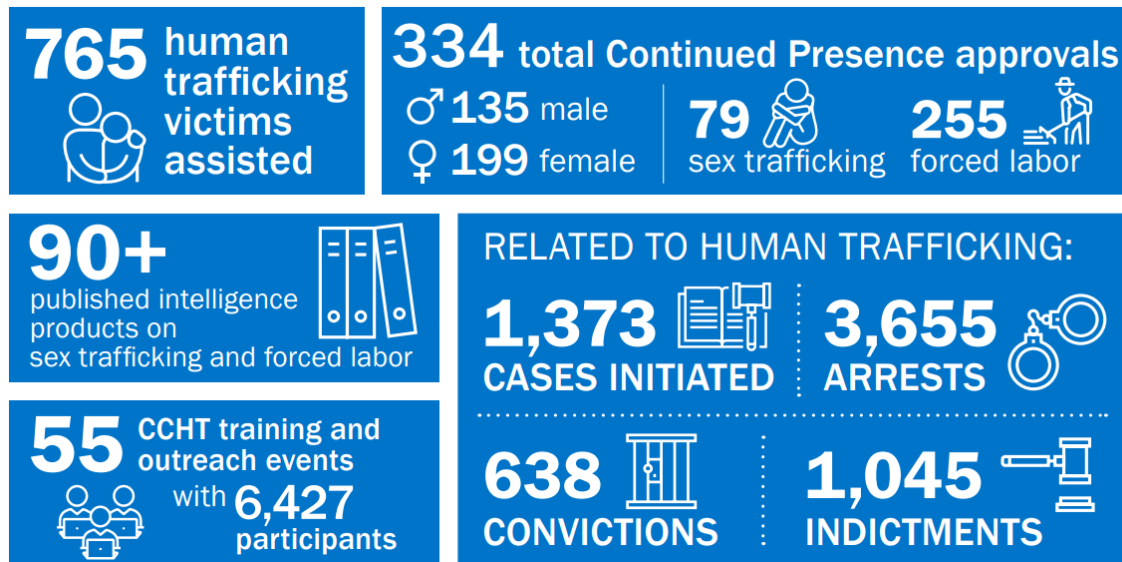
<b>1. INTRODUCTION</b>	<b>6</b>
1.1 RELEVANT EU LEGISLATIVE INITIATIVES	6
1.2 THE ROLE OF DATA PROTECTION ENGINEERING	7
1.3 SCOPE AND OBJECTIVES	7
1.4 STRUCTURE OF THE DOCUMENT	8
<b>2. DATA SHARING PRACTICES IN THE HEALTH SECTOR</b>	<b>9</b>
2.1 USER CONTROLLED PERSONAL DATA SHARING	9
2.1.1 Attribute Based Encryption	11
2.1.2 Proxy Re-encryption	12
2.2 SHARING HEALTH DATA FOR MEDICAL AND RESEARCH PURPOSES BY HEALTH CARE PROVIDERS	13
2.2.1 Polymorphic encryption and pseudonymisation	13
<b>3. DATA SHARING USING THIRD-PARTY SERVICES</b>	<b>15</b>
3.1 MOBILE PUSH NOTIFICATIONS	15
3.1.1 Anonymous Notification Protocols (Using Proxies)	17
3.1.2 End-to-End Encryption	18
3.1.3 Design Strategies	18
3.2 DATA SHARING DURING AUTHENTICATION	19
3.2.1 Relevance of attribute based access to online platforms	20
<b>4. CONSIDERATIONS ON EXERCISING THE RIGHTS OF DATA SUBJECTS</b>	<b>22</b>
4.1 INTERACTION BETWEEN DATA SUBJECT AND DATA INTERMEDIARY	24
4.1.1 Purpose Limitations	24
4.1.2 Implementation Aspects	25
4.2 INTERACTION BETWEEN DATA INTERMEDIARY AND DATA UTILISERS	25
4.2.1 Data Request and Data Response	25
4.3 DATA MANAGEMENT AT THE DATA INTERMEDIARY	26
4.3.1 Consent Coverage and Purpose Limitation	26
4.3.2 Inter-Intermediary Interaction	27
4.3.3 Logging and Reporting	28
4.3.4 Privacy-Preserving Data Selection	28
4.4 DATA ALTRUISM	28
<b>5. CONCLUSIONS</b>	<b>29</b>
<b>REFERENCES</b>	<b>30</b>

*Number 7***Countering Human Trafficking Year in Review**

U.S. Department of Homeland Security (DHS)

**Homeland Security****Center for Countering Human Trafficking**

The DHS Countering Human Trafficking Year in Review reports on select accomplishments and advancements made by U.S. Department of Homeland Security (DHS) offices and components towards countering human trafficking. These annual reports include links to additional informative resources that explain DHS's counter-trafficking operations, outreach, and other efforts.

**HOMELAND SECURITY INVESTIGATIONS**

Human trafficking is a crime of exploiting another person for compelled labor or commercial sex acts, typically through force, fraud, or coercion, or by inducing a minor under 18 into commercial sex.

According to the United Nations' International Labour Organization, human traffickers victimize an estimated 28 million people worldwide, with 80% subjected to forced labor and 20% in sex trafficking.

The United States is no exception. Many trafficking cases in the United States involve workers in agriculture, landscaping, construction, factories, in homes as nannies or other domestic workers, restaurants, elder care, massage parlors, and more — essentially in jobs with low pay and few legal protections in the underground economy and the service industry.

Combating human trafficking is a top priority for the U.S. Department of Homeland Security (DHS).

In 2020, the Secretary of DHS released the DHS Strategy to Combat Human Trafficking, the Importation of Goods Produced with Forced Labor, and Child Sexual Exploitation (“the Strategy”). You may visit: [https://www.dhs.gov/sites/default/files/publications/20\\_0115\\_plcy\\_hum-an-trafficking-forced-labor-child-exploit-strategy.pdf](https://www.dhs.gov/sites/default/files/publications/20_0115_plcy_hum-an-trafficking-forced-labor-child-exploit-strategy.pdf)

## DEPARTMENT OF HOMELAND SECURITY STRATEGY TO COMBAT HUMAN TRAFFICKING, THE IMPORTATION OF GOODS PRODUCED WITH FORCED LABOR, AND CHILD SEXUAL EXPLOITATION



It represents the DHS vision to end this urgent humanitarian issue, articulates the Department’s long-term approach for combating these crimes, and serves as a framework to prioritize our resources and monitor progress.

You may visit: [https://www.dhs.gov/sites/default/files/2023-01/23\\_0131\\_CCHT\\_year-in-review.pdf](https://www.dhs.gov/sites/default/files/2023-01/23_0131_CCHT_year-in-review.pdf)

*Number 8***ECONOMIC AND NATIONAL SECURITY IMPLICATIONS OF THE COVID-19 PANDEMIC THROUGH 2026**

Office of the  
Director of National Intelligence



DECLASSIFIED by DNI Haines on 14 January 2023

**NATIONAL  
INTELLIGENCE  
ESTIMATE**

April 2022

NIE 2022-02480

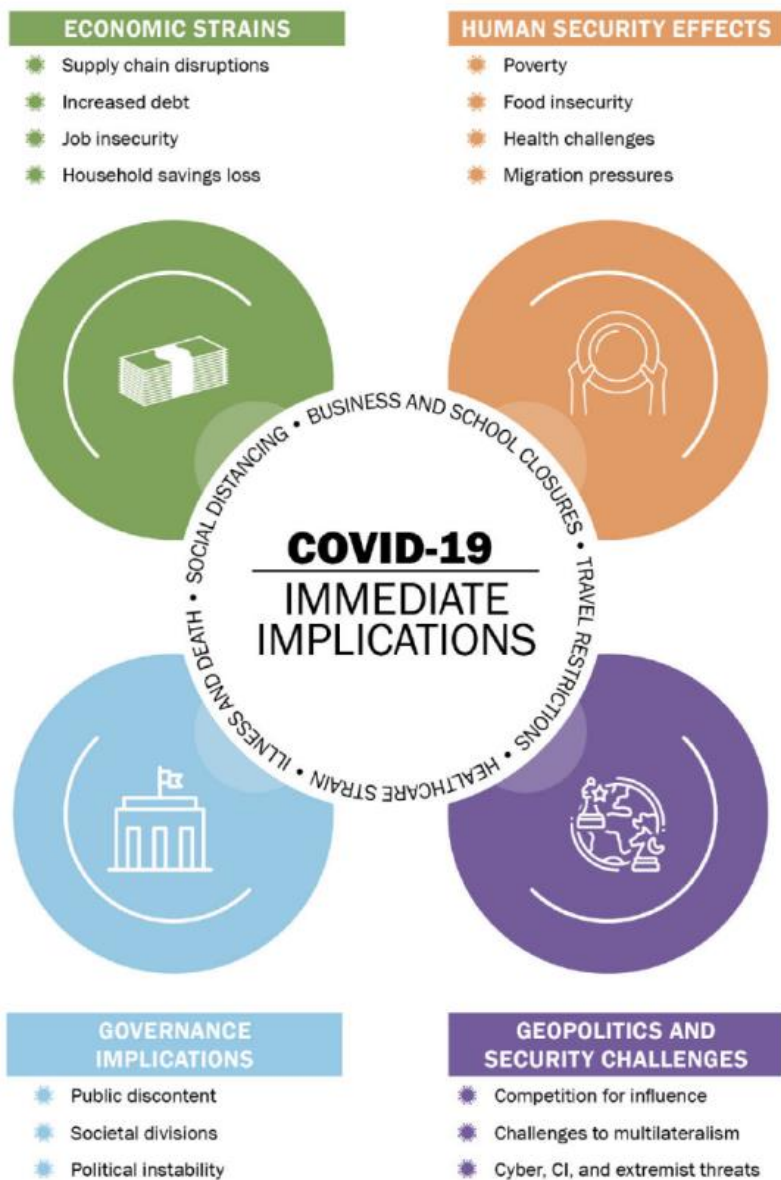
**(U [REDACTED]) Economic and National  
Security Implications of the COVID-  
19 Pandemic Through 2026**

(U [REDACTED]) **Key Judgment 1: Economics.** During the next five years, as most countries recover from the most severe economic effects of COVID-19, we assess that pandemic-related higher debt burdens, constrained government spending, and ongoing disruptions to the labor market probably will contribute to higher risks of financial instability and elevated rates of poverty, particularly in developing countries. Most advanced economies are better positioned to recover economically from the effects of COVID-19 because they had early and widespread access to vaccines and have a greater ability to apply and sustain supportive monetary and fiscal policies.

(U [REDACTED]) **Key Judgment 2: Human Security.** The COVID-19 pandemic and its economic fallout are likely to continue to have harmful effects for human security—the protection of individuals from threats to their well-being—during the next five years, while stimulating some improvements in global preparedness for future pandemics.

(U [REDACTED]) **Key Judgment 3: Governance.** Through 2026, the combination of economic and human security challenges resulting from the COVID-19 pandemic is likely to further strain the capacities of governments to meet public demands, thereby exacerbating existing public discontent and societal divisions, and raising the risks to democratic governance and political stability in some countries.

[REDACTED] **Key Judgment 4: Geopolitics.** The pandemic is likely to continue to be exploited by US adversaries to build their influence, probably with limited success; to encourage some US partners and allies to prioritize domestic and regional needs over addressing other international challenges; and to drive initiatives to improve multilateral mechanisms to address health security and other transnational issues.



### (U) Key Takeaway

During the next five years, the COVID-19 pandemic is likely to exacerbate a range of global economic, human security, governance, and geopolitical strains, even as the pandemic's most severe health effects are likely to fade. Developing countries probably will face the most critical and enduring socioeconomic setbacks, which are likely to contribute to increasing humanitarian needs, political instability, and geopolitical tensions. Most advanced economies are likely to be able to manage longer-term economic disruptions, in part because they were able to implement early and aggressive fiscal and monetary measures.

This NIE was written with a high degree of uncertainty because of the unprecedented and ongoing nature of the health crisis, including the continual emergence of new variants, such as Omicron, and the high levels of vaccine hesitancy globally. We made baseline assumptions about the trajectory of the virus during the next five years to ground our judgments of the broader implications. We assume that the virus that causes COVID-19 will continue to circulate globally during the next five years. For most countries, the most severe health effects of the pandemic are likely to abate during the next year as vaccination coverage expands, immunity from infections builds, and the availability and effectiveness of therapeutics grow.

## (U) Annex B: Misinformation Likely To Continue Damaging Public Health Communications

---

■■■■■ We assess that US adversaries and local actors worldwide are likely to continue using social media-driven information environments to spread misinformation about COVID-19 and future infectious disease outbreaks in ways that probably will increase publics' hesitancy to be vaccinated, undercut governments' abilities to effectively promote public health, and stoke social discord. We assess that public health communicators are struggling to compete with misinformation actors in part because social media algorithms often favor emotionally compelling content, which is easier for audiences to process than complex, evidence-based health guidance■■■■■

■■■■■

- (U) By the end of 2020, a COVID-19 misinformation-tracking project had identified nearly 6,000 narratives across 80 countries, with social media by far the most common means of sharing misinformation. Researchers who examined COVID-19 information circulating on social media in 2020 found that misinformation received six times more “likes,” shares, and interactions on Facebook than more authoritative sources, such as the WHO. People who get information solely from social media are more susceptible to COVID-19 misinformation, leading them to be less likely to follow safety protocols, get vaccinated, or encourage others to get vaccinated, according to an academic study of populations in Ireland, Mexico, Spain, the United Kingdom, and the United States.

To read more:

[https://www.dni.gov/files/ODNI/documents/assessments/NIE-Economic and National Security Implications of the COVID-19 Pandemic Through 2026.pdf](https://www.dni.gov/files/ODNI/documents/assessments/NIE-Economic%20and%20National%20Security%20Implications%20of%20the%20COVID-19%20Pandemic%20Through%202026.pdf)

*Number 9*

## How Cybersecurity Standards Support the Evolving EU Legislative Landscape



The European Union Agency for Cybersecurity (ENISA) joined forces with the European Standards Organisations (ESOs), CEN, CENELEC and ETSI, to organise their 7th annual conference. The hybrid conference focused on "European Standardisation in support of the EU cybersecurity legislation".



Given the latest developments in cybersecurity policy, the hybrid conference focused once more on European Standardisation in support of EU cybersecurity legislation. Building on the effective contributions of past editions, the high-level event attracted over 1600 attendees from the European Union and from the international sphere.

The conference was organised around four panels, which discussed ongoing standardisation work and future requirements. The event opened by the European Standards Organisations, Ms. Elena Santiago Cid, Director General of CEN and CENELEC, Mr. Wolfgang Niedziella, President of CENELEC, Mr. Luis Jorge Romero, ETSI Director-General and Mr. Andreas Mitrakas, head of unit "Market Certification and



Standardisation" at ENISA, as well as Ms. Christiane Kirketerp de Viron, head of unit Cybersecurity and Digital Privacy Policy at the European Commission.

The first panel addressed the future of EU standardisation with the "regional versus international" angle.

The second panel dealt with the **Cyber Resilience Act (CRA)** as a game changer and how standards can support it.

The **Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (or eIDAS) V2** and digital identities were the topics of the third panel, while the final panel gave an overview of the landscape of the EU cybersecurity legislation.

Participants came from a diverse community of associations representing small and medium enterprises and vertical sectors, industry, and included several speakers from the European Commission.

To read more: <https://www.enisa.europa.eu/news/how-cybersecurity-standards-support-the-evolving-eu-legislative-landscape>

*Number 10***(De)globalisation and economic policies in the European context**

Pablo Hernández de Cos, Governor of the Bank of Spain, at the Dialogue with the Governor on the Future of Globalisation, Cañada Blanch Centre for Contemporary Spanish Studies and London School of Economics and Political Science, London.



Let me start by thanking Professor Andrés Rodríguez-Pose, the Cañada Blanch Centre for Contemporary Spanish Studies of the London School of Economics (LSE) and the LSE for their kind invitation, and for giving me the opportunity to hold this dialogue with you on a fascinating topic: the future of globalisation.

The questions currently surrounding this topic are of the utmost importance for highly open and integrated economies, such as the euro area and the UK.

The two extraordinary shocks that have recently hit the global economy, the Covid-19 pandemic and, above all, the Russian invasion of Ukraine, have disrupted global value chains and commodity markets, and generated an environment of heightened uncertainty and geopolitical tensions.

Added to the past and present episodes of trade tensions between the US and China, among others, these shocks have prompted renewed questions regarding the future of globalisation and the increasing importance of geopolitical factors in shaping international economic relations.

Although the globalisation of goods was slowing down even before the pandemic, concerns about the resilience of global value chains and the supply security of strategic products are now becoming more apparent in decisions made by firms and policy measures considered by governments.

For their part, governments have become more concerned that trade and financial openness may create dependencies on third countries that increase vulnerability to geopolitical shocks.

Accordingly, they have started to include geopolitical considerations in their economic decision-making, with policy initiatives that aim to limit such external vulnerabilities, for example, by encouraging the local

production of strategic products such as semiconductors or by screening incoming foreign direct investment on grounds of national security.

These issues are particularly important for the EU, given its high degree of trade and financial openness, which is larger than that of other geopolitical powers such as the United States or China.

For example, in 2019 the share of foreign trade reached 54% of GDP in the euro area (up from 31% in 1999), which is double that of the US (26%), while the share of global value chain participation in trade is 20 percentage points higher in the euro area than in the United States.

Likewise, the euro area is more financially open than the US, as measured by the stock of gross external assets and liabilities with respect to GDP.

This openness has been a major advantage for Europe for many years and one of the main reasons for its prosperity.

This openness has allowed the EU to benefit from lower import prices, larger export opportunities, more foreign competition, technology diffusion and, ultimately, productivity gains.

But it has also become an element of vulnerability in a more volatile global geopolitical environment. This is currently evident in the EU's external energy dependence.

In this context, I would like to focus my speech today on three issues. I will begin by focusing on the implications of the changing patterns of globalisation for the European economy.

In particular, I will provide an analysis of the vulnerabilities and dependencies affecting the EU's trade and financial flows, based on a report soon to be published by the Eurosystem.

In the second section, I will take stock of the European policy response to reduce those vulnerabilities and exposures and the dilemmas it faces. I will also provide some insights into how I think European policies should react.

In the last part of my talk, I will focus on the implications of this trend for the ECB's monetary policy.

In its recent strategy review, the ECB looked carefully at the consequences of globalisation for the conduct of monetary policy.

The obvious question is whether we should now expect similar effects with opposite sign as a result of a possible increase in fragmentation.

## *EU vulnerabilities in a globalised environment*

The EU is deeply integrated into the global economy and has strong links with other major geopolitical powers, such as the US in terms of finance and trade, China in terms of trade and, before the war, Russia in terms of energy and raw materials supply.

What are the main vulnerabilities observed as a consequence of this high degree of integration?

One source of vulnerability in the face of rising geopolitical tensions is Europe's high external dependency with respect to some products which are key to the EU economy, but which are imported from a handful of non-EU countries.

China accounts for a large share of goods imports into the EU. China is also the main exporter to the EU of several electronic products (such as computers and optical devices), for which domestic production capacity is also relatively low.

This situation is not unique to the EU. As a consequence, China is becoming the "OPEC of industrial inputs".

This dependence on Chinese imports already had significant consequences for the European manufacturing sector during the pandemic.

There is evidence that the Chinese supply chain disruptions that occurred in the early months of the pandemic had a considerable impact on manufacturing output in the euro area, temporarily reducing it by 7%.

The EU is also dependent on third countries for semiconductor production.

European companies involved in the manufacture of these products concentrate almost exclusively on the upstream stage of the production chain, providing manufacturing equipment and high-purity materials used in chip production.

However, European companies account for a negligible share of other critical stages of the production chain, such as chip design or assembly.

They are also heavily dependent on foreign suppliers: almost 80% of the suppliers of European semiconductor companies are based outside the EU. To read more:

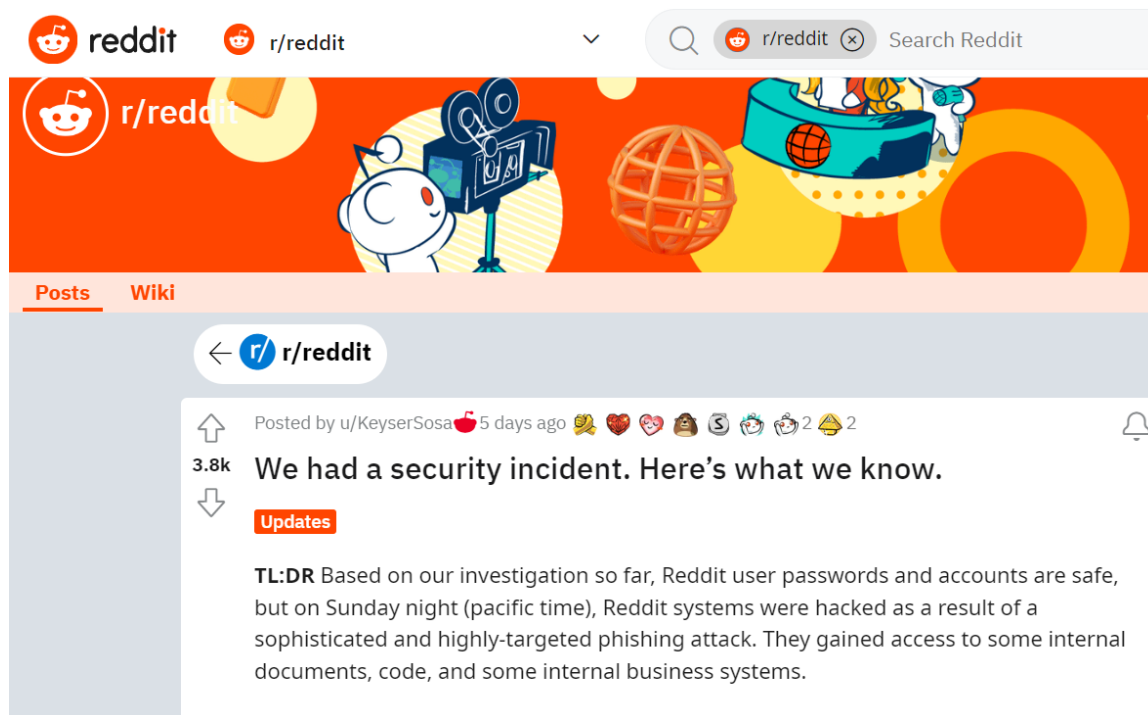
<https://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/IntervencionesPublicas/Gobernador/Arc/Fic/IIPP-2023-02-09-hdc-en.pdf>

## *Number 11*

We had a security incident. Here's what we know.



**TL:DR** Based on our investigation so far, Reddit user passwords and accounts are safe, but on Sunday night (pacific time), Reddit systems were hacked as a result of a sophisticated and highly-targeted phishing attack. They gained access to some internal documents, code, and some internal business systems.



### *What Happened?*

On late (PST) February 5, 2023, we became aware of a sophisticated **phishing** campaign that targeted Reddit employees. As in most phishing campaigns, the attacker sent out plausible-sounding prompts pointing employees to a website that cloned the behavior of our intranet gateway, in an attempt to steal credentials and second-factor tokens.

After successfully obtaining a **single** employee's credentials, the attacker gained access to some internal docs, code, as well as some internal dashboards and business systems. We show no indications of breach of our primary production systems (the parts of our stack that run Reddit and store the majority of our data).

Exposure included limited contact information for (currently hundreds of) company contacts and employees (current and former), as well as limited advertiser information. Based on several days of initial investigation by

security, engineering, and data science (and friends!), we have no evidence to suggest that any of your non-public data has been accessed, or that Reddit's information has been published or distributed online.

### *How Did We Respond?*

Soon after being phished, the affected employee self-reported, and the Security team responded quickly, removing the infiltrator's access and commencing an internal investigation.

Similar phishing attacks have been recently reported. We're continuing to investigate and monitor the situation closely and working with our employees to fortify our security skills. As we all know, the human is often the weakest part of the security chain.

Our goal is to fully understand and prevent future incidents of this nature, and we will use this post to provide any additional updates as we learn and can share more. So far, it also appears that many of the lessons we learned five years ago have continued to be useful.

### *User Account Protection*

Since we're talking about security and safety, this is a good time to remind you how to protect your Reddit account. The most important (and simple) measure you can take is to set up 2FA (two-factor authentication) which adds an extra layer of security when you access your Reddit account. Learn how to enable 2FA in Reddit Help. And if you want to take it a step further, it's always a good idea to update your password every couple of months – just make sure it's strong and unique for greater protection.

Also: use a password manager! Besides providing great complicated passwords, they provide an extra layer of security by warning you before you use your password on a phishing site... because the domains won't match!

To read more:

[https://www.reddit.com/r/reddit/comments/10y427y/we\\_had\\_a\\_security\\_incident\\_heres\\_what\\_we\\_know/](https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/)

*Number 12*

## Screentime: Sometimes It Feels Like Somebody's Watching Me **proofpoint.**

Since October 2022 and continuing into January 2023, Proofpoint has observed a cluster of evolving financially motivated activity which we are referring to as "Screentime".

The attack chain starts with an email containing a malicious attachment or URL and leads to malware that Proofpoint dubbed WasabiSeed and Screenshotter. In some cases, Proofpoint observed post-exploitation activity involving AHK Bot and Rhadamanthys Stealer.

Proofpoint is tracking this activity under threat actor designation TA866. Proofpoint assesses that TA866 is an organized actor able to perform well thought-out attacks at scale based on their availability of custom tools; ability and connections to purchase tools and services from other vendors; and increasing activity volumes.

To read more: <https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me>



*Number 13***Predicting pandemics through museum animal collections**

Coalition studies UNM museum samples to explore pathogens



Zoonotic pathogens, those that spill over from animals to humans such as SARS-CoV-2 and hantavirus, present a challenge for scientists in terms of how the diseases evolve and spread in animal populations.

Now, a broad coalition of institutions, including Los Alamos National Laboratory and the University of New Mexico, seeks to shed light on the evolution and spread of these pathogens before they make the jump into human populations.

“Our understanding of pathogens with high spill-over potential is limited by our preference for sampling human cases after a spill-over has already happened,” said Ethan Romero-Severson, a Los Alamos co-lead on the project. “This type of reactive data collection limits our ability to see the clues as to what was going on in the animal populations before the spill-over occurred.”

The central innovation behind the coalition — called the Pathogen Informatics Center for Analysis, Networking, Translation & Education (PICANTE) — directly addresses this deficiency by using the extensive frozen animal-tissue biorepositories housed at natural history museums around the globe. In fact, the most extensive collection of cryopreserved mammalian tissue known to date is housed at UNM’s Museum of Southwestern Biology (MSB).

PICANTE is currently funded through a Phase 1 Predictive Intelligence for Pandemic Preparedness (PIPP) grant from the National Science Foundation.

*Premier datasets allow scientists to study host-pathogen relationships*

Using the preserved tissues at MSB and those from collaborating biorepositories, scientists in PICANTE can develop screening and genetic sequencing methods to isolate pathogens from these extensive collections.

Because the data has been curated and vouchsafed by museums such as MSB over a period of decades, scientists have access to datasets spanning both space and time, resources that would be impossible to collect without the foresight of the collaborators at MSB.



The Los Alamos team includes Romero-Severson and Emma Goldberg, whose role in PICANTE is to develop methods for studying the evolutionary relationships among hosts and pathogens. They will also use pathogen sequence data coming from these biorepositories to document the history of pathogens such as hantavirus jumping between different rodent species.

“If we can understand what allows or inhibits pathogens to move between different animal species, we can better understand the risk animal pathogens pose to human health and global security,” said Romero-Severson.

“Despite being a small state, we have a golden opportunity here in New Mexico: UNM has the world’s largest collection of cryopreserved mammalian tissues coupled to an extensive network of international biorepositories, and Los Alamos has decades-long experience developing the methodology to model the evolution, epidemiology and control of pathogens and the computational power to actually implement those methods.”

Romero-Severson added, “PICANTE offers a new way for Los Alamos and UNM scientists to collaborate on some of the most pressing questions that will dominate the intersection of public health and global security in the coming decades.”

To read more: <https://discover.lanl.gov/news/0210-picante/>

## *Number 14*

### U.S. Department of Justice Disrupts Hive Ransomware Variant FBI Covertly Infiltrated Hive Network, Thwarting Over \$130 Million in Ransom Demands



The Justice Department announced today its months-long disruption campaign against the Hive ransomware group that has targeted more than 1,500 victims in over 80 countries around the world, including hospitals, school districts, financial firms, and critical infrastructure.

Since late July 2022, the FBI has penetrated Hive's computer networks, captured its decryption keys, and offered them to victims worldwide, preventing victims from having to pay \$130 million in ransom demanded.

Since infiltrating Hive's network in July 2022, the FBI has provided over 300 decryption keys to Hive victims who were under attack. In addition, the FBI distributed over 1,000 additional decryption keys to previous Hive victims.

Finally, the department announced today that, in coordination with German law enforcement (the German Federal Criminal Police and Reutlingen Police Headquarters-CID Esslingen) and the Netherlands National High Tech Crime Unit, it has seized control of the servers and websites that Hive uses to communicate with its members, disrupting Hive's ability to attack and extort victims.

"Last night, the Justice Department dismantled an international ransomware network responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world," said Attorney General Merrick B. Garland.

"Cybercrime is a constantly evolving threat. But as I have said before, the Justice Department will spare no resource to identify and bring to justice, anyone, anywhere, who targets the United States with a ransomware attack. We will continue to work both to prevent these attacks and to provide support to victims who have been targeted. And together with our international partners, we will continue to disrupt the criminal networks that deploy these attacks."

“The Department of Justice’s disruption of the Hive ransomware group should speak as clearly to victims of cybercrime as it does to perpetrators,” said Deputy Attorney General Lisa O. Monaco.

“In a 21st century cyber stakeout, our investigative team turned the tables on Hive, swiping their decryption keys, passing them to victims, and ultimately averting more than \$130 million dollars in ransomware payments. We will continue to strike back against cybercrime using any means possible and place victims at the center of our efforts to mitigate the cyber threat.”

“The coordinated disruption of Hive’s computer networks, following months of decrypting victims around the world, shows what we can accomplish by combining a relentless search for useful technical information to share with victims with investigation aimed at developing operations that hit our adversaries hard,” said FBI Director Christopher Wray.

“The FBI will continue to leverage our intelligence and law enforcement tools, global presence, and partnerships to counter cybercriminals who target American business and organizations.”

“Our efforts in this case saved victims over a hundred million dollars in ransom payments and likely more in remediation costs,” said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department’s Criminal Division.

“This action demonstrates the Department of Justice’s commitment to protecting our communities from malicious hackers and to ensuring that victims of crime are made whole. Moreover, we will continue our investigation and pursue the actors behind Hive until they are brought to justice.”

“Cybercriminals utilize sophisticated technologies to prey upon innocent victims worldwide,” said U.S. Attorney Roger Handberg for the Middle District of Florida.

“Thanks to the exceptional investigative work and coordination by our domestic and international law enforcement partners, further extortion by HIVE has been thwarted, critical business operations can resume without interruption, and millions of dollars in ransom payments were averted.”

Since June 2021, the Hive ransomware group has targeted more than 1,500 victims around the world and received over \$100 million in ransom payments.

Hive ransomware attacks have caused major disruptions in victim daily operations around the world and affected responses to the COVID-19 pandemic.

In one case, a hospital attacked by Hive ransomware had to resort to analog methods to treat existing patients and was unable to accept new patients immediately following the attack.

Hive used a ransomware-as-a-service (RaaS) model featuring administrators, sometimes called developers, and affiliates. RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims.

Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.

Hive actors employed a double-extortion model of attack. Before encrypting the victim system, the affiliate would exfiltrate or steal sensitive data. The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data.

Hive actors frequently targeted the most sensitive data in a victim's system to increase the pressure to pay. After a victim pays, affiliates and administrators split the ransom 80/20. Hive published the data of victims who do not pay on the Hive Leak Site.

According to the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Hive affiliates have gained initial access to victim networks through a number of methods, including: single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols; exploiting FortiToken vulnerabilities; and sending phishing emails with malicious attachments.

To read more: <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>

*Number 15*

## Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay \$30 Million to Settle SEC Charges



The Securities and Exchange Commission charged Payward Ventures, Inc. and Payward Trading Ltd., both commonly known as Kraken, with failing to register the offer and sale of their crypto asset staking-as-a-service program, whereby investors transfer crypto assets to Kraken for staking in exchange for advertised annual investment returns of as much as 21 percent.

To settle the SEC's charges, the two Kraken entities agreed to immediately cease offering or selling securities through crypto asset staking services or staking programs and pay \$30 million in disgorgement, prejudgment interest, and civil penalties.

According to the SEC's complaint, since 2019, Kraken has offered and sold its crypto asset "staking services" to the general public, whereby Kraken pools certain crypto assets transferred by investors and stakes them on behalf of those investors.

Staking is a process in which investors lock up – or "stake" – their crypto tokens with a blockchain validator with the goal of being rewarded with new tokens when their staked crypto tokens become part of the process for validating data for the blockchain.

When investors provide tokens to staking-as-a-service providers, they lose control of those tokens and take on risks associated with those platforms, with very little protection.

The complaint alleges that Kraken touts that its staking investment program offers an easy-to-use platform and benefits that derive from Kraken's efforts on behalf of investors, including Kraken's strategies to obtain regular investment returns and payouts

"Whether it's through staking-as-a-service, lending, or other means, crypto intermediaries, when offering investment contracts in exchange for investors' tokens, need to provide the proper disclosures and safeguards required by our securities laws," said SEC Chair Gary Gensler.

“Today’s action should make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection.”

“In case after case, we’ve seen the consequences when individuals and businesses tout and offer crypto investments outside of the protections provided by the federal securities laws: investors lack the disclosures they deserve and are harmed when they don’t receive them,” said Gurbir S. Grewal, Director of the SEC’s Division of Enforcement.

“Today, we take another step in protecting retail investors by shutting down this unregistered crypto staking program, through which Kraken not only offered investors outsized returns untethered to any economic realities, but also retained the right to pay them no returns at all. All the while, it provided them zero insight into, among other things, its financial condition and whether it even had the means of paying the marketed returns in the first place.”

In addition to ceasing the staking program and the monetary relief, Payward Ventures, Inc. and Payward Trading, Ltd, without admitting or denying the allegations in the SEC’s complaint, consented to the entry of a final judgment, subject to court approval, that would permanently enjoin each of them from violating Section 5 of the Securities Act of 1933 and permanently enjoin them and any entity they control from, directly or indirectly, offering or selling securities through crypto asset staking services or staking programs.

The SEC’s investigation was conducted by Laura D’Allaird and Elizabeth Goody, under the supervision of Paul Kim, Jorge G. Tenreiro, and David Hirsch, with assistance from Sachin Verma, Eugene Hansen, and James Connor.

To read more: <https://www.sec.gov/news/press-release/2023-25>

*Number 16*

## Statement

**Kraken Down: Statement on SEC v. Payward Ventures, Inc., et al.**  
SEC Commissioner Hester M. Peirce

Today, the SEC shut down Kraken’s staking program and counted it as a win for investors. I disagree and therefore dissent.

Kraken operated a service through which its customers could offer their tokens up for staking. The customers earned returns, and the company earned a fee. The Commission argues that this staking program should have been registered with the SEC as a securities offering.

Whether one agrees with that analysis or not, the more fundamental question is whether SEC registration would have been possible. In the current climate, crypto-related offerings are not making it through the SEC’s registration pipeline.

An offering like the staking service at issue here raises a host of complicated questions, including whether the staking program as a whole would be registered or whether each token’s staking program would be separately registered, what the important disclosures would be, and what the accounting implications would be for Kraken.

We have known about crypto staking programs for a long time. Although it may not have made a difference, I should have called for us to put out guidance on staking long before now.

Instead of taking the path of thinking through staking programs and issuing guidance, we again chose to speak through an enforcement action, purporting to “make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection.”

Using enforcement actions to tell people what the law is in an emerging industry is not an efficient or fair way of regulating.

Moreover, staking services are not uniform, so one-off enforcement actions and cookie-cutter analysis does not cut it.

Most concerning, though, is that our solution to a registration violation is to shut down entirely a program that has served people well. The program will no longer be available in the United States, and Kraken is enjoined from ever offering a staking service in the United States, registered or not.

A paternalistic and lazy regulator settles on a solution like the one in this settlement: do not initiate a public process to develop a workable registration process that provides valuable information to investors, just shut it down.

More transparency around crypto-staking programs like Kraken's might well be a good thing. However, whether we need a uniform regulatory solution and if that regulatory solution is best provided by a regulator that is hostile to crypto, in the form of an enforcement action, is less clear.

To read more: <https://www.sec.gov/news/statement/peirce-statement-kraken-020923>



*Number 17***An important next step on our AI journey**

Sundar Pichai, CEO of Google and Alphabet



AI is the most profound technology we are working on today. Whether it's helping doctors detect diseases earlier or enabling people to access information in their own language, AI helps people, businesses and communities unlock their potential. And it opens up new opportunities that could significantly improve billions of lives.

That's why we re-oriented the company around AI six years ago — and why we see it as the most important way we can deliver on our mission: to organize the world's information and make it universally accessible and useful.

Since then we've continued to make investments in AI across the board, and Google AI and DeepMind are advancing the state of the art. Today, the scale of the largest AI computations is doubling every six months, far outpacing Moore's Law. At the same time, advanced generative AI and large language models are capturing the imaginations of people around the world.

In fact, our Transformer research project and our field-defining paper in 2017, as well as our important advances in diffusion models, are now the basis of many of the generative AI applications you're starting to see today.

***Introducing Bard***

It's a really exciting time to be working on these technologies as we translate deep research and breakthroughs into products that truly help people. That's the journey we've been on with large language models.

Two years ago we unveiled next-generation language and conversation capabilities powered by our Language Model for Dialogue Applications (or LaMDA for short).

We've been working on an experimental conversational AI service, powered by LaMDA, that we're calling Bard. And today, we're taking another step forward by opening it up to trusted testers ahead of making it more widely available to the public in the coming weeks.

Bard seeks to combine the breadth of the world's knowledge with the power, intelligence and creativity of our large language models. It draws on information from the web to provide fresh, high-quality responses.

Bard can be an outlet for creativity, and a launchpad for curiosity, helping you to explain new discoveries from NASA's James Webb Space Telescope to a 9-year-old, or learn more about the best strikers in football right now, and then get drills to build your skills.

To read more: <https://blog.google/technology/ai/bard-google-ai-search-updates/>

## *Number 18*

### Applying AI to some of the world's biggest challenges



At Google, we believe that AI can provide new ways of approaching problems and meaningfully improve people's lives. With AI, we have another tool to explore and address hard, unanswered questions. What if people could predict natural disasters before they happen? Track disease as it spreads, to eliminate it sooner? Or dramatically improve the lives of people with disabilities?

AI can help, but it's not a silver bullet: tackling these questions requires a concerted, collaborative effort across all sectors of society. At Google, we believe that we can meaningfully contribute, drawing on the scale of our products and services, investment in AI research, and our commitment to using and developing AI responsibly. We're doing that through AI for Social Good, a program that focuses Google's AI expertise on solving humanitarian and environmental challenges.

Our work through the program centers around supporting core research and engineering efforts and empowering the social sector with tools, resources and funding, while engaging with partners across all sectors to have the biggest impact. Further, we are tackling problems within public health, nature & society, climate & energy, accessibility and crisis response.

We also strongly believe the ability to find these solutions relies on the expertise of people around the world. That's why we've opened up research centers in Japan, India, Israel, and Accra and are also partnering with nonprofits, academia and public sector organizations to create systemic solutions.

#### *Why we focus on AI (and to what end)*

We believe that AI, including its core methods such as machine learning (ML), is a foundational and transformational technology.

AI enables innovative new uses of tools, products, and services, and it is used by billions of people every day, as well as businesses, governments, and other organizations.

AI can assist, complement, empower, and inspire people in almost every field, from everyday tasks to bold and imaginative endeavors.

It can unlock new scientific discoveries and opportunities, and help tackle humanity's greatest challenges—today and in the future.

As many have highlighted, we believe that AI has the potential to benefit people and society through its capacity to:

- Make information more useful and available to more people, everywhere, often helping overcome barriers including access, disabilities and language
- Assist people and organizations to make decisions, solve problems, be more productive and creative in their daily and work lives
- Enable innovation that leads to new, helpful products and services for people, organizations, and society more broadly
- Help tackle current and pressing real world challenges, such as public health crises, natural disasters, climate change, and sustainability
- Help identify and mitigate societal biases and structural inequities (e.g. socio-economic, sociodemographic and regional inequities)
- Enable scientific and other breakthroughs to address humanity's greatest future opportunities and challenges (e.g. medical diagnosis, drug discovery, climate forecasting).

To read more: <https://ai.google/social-good/>

<https://ai.google/static/documents/google-why-we-focus-on-ai.pdf>

*Number 19*

## The future of AI is now



Introducing the new Bing - Ask real questions, get complete answers, and turn ideas into content with Bing—your AI-powered copilot for the web.

Help me plan a trip to London

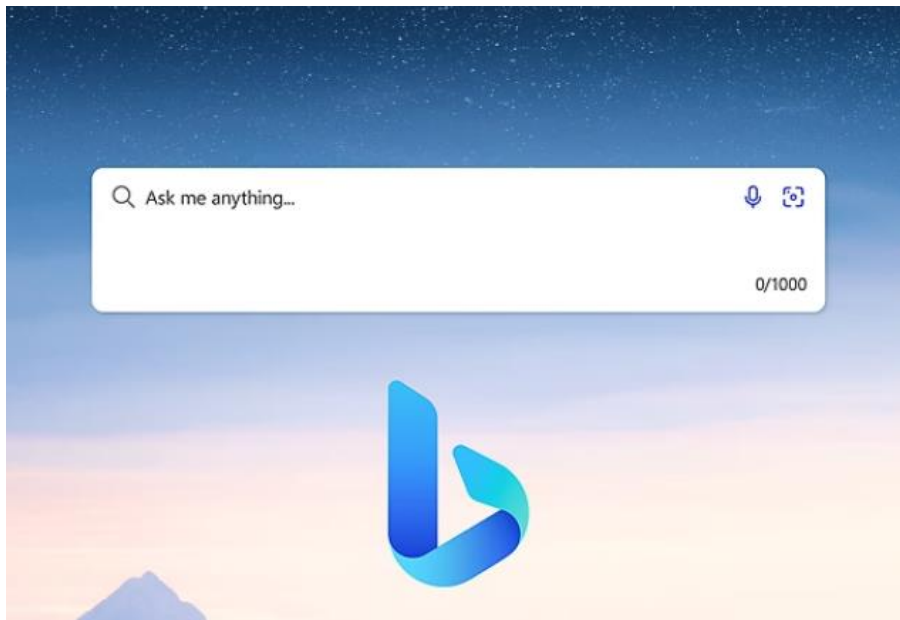
✓ Generating answers for you...

Sure, I can help you plan a trip to London. London is a great city to visit, with iconic attractions, historic museums, and vibrant neighborhoods. You can find things to do in London, from sightseeing tours to fun-filled days out, on [visitlondon.com](#) <sup>1</sup>. You can also book a London Pass to make the most of popular attractions <sup>2</sup> or a one-day hop-on hop-off bus tour to explore the sights at your own pace <sup>3</sup>. You can find cheap flights to London from \$99 on [KAYAK](#) <sup>4</sup> and London vacation packages from \$849 on [Expedia](#) <sup>5</sup>.

When is the best time to visit

✓ Generating answers for you...

The best time to visit London depends on your preferences and budget, but generally speaking, the **spring** (March to May) and the **autumn** (September to November) are the most pleasant seasons, with mild temperatures, green and blooming parks, and fewer crowds than the summer (June to August). <sup>1 2 3</sup> The **summer** is also a popular time to visit, with warm and sunny weather, but also higher prices and more tourists. <sup>1 2</sup> The **winter** (December to February) is the coldest and wettest season, but also offers festive attractions, lower rates, and fewer queues. <sup>2 4</sup>

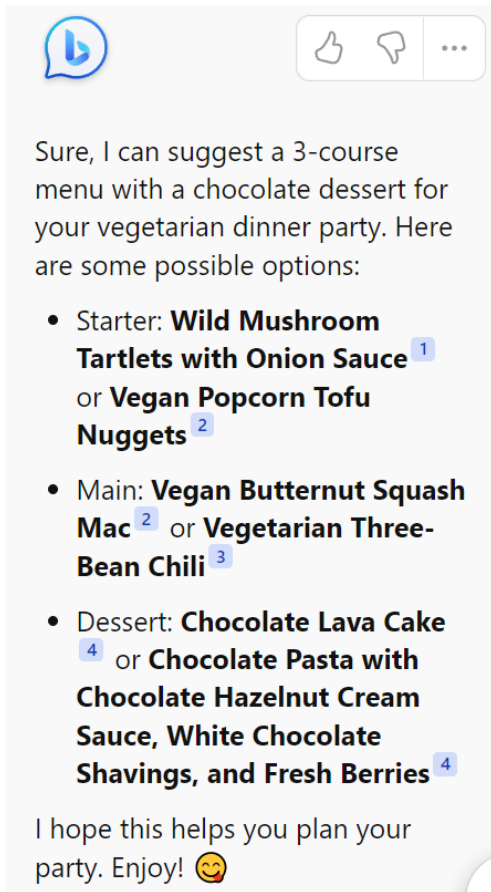


## What art ideas can I do with my kid?

I found some **arts and crafts ideas** for a toddler using only cardboard boxes, plastic bottles, paper and string. Here are some examples:

- You can make a **cardboard box guitar** with a tissue box, a cardboard tube, some rubber bands, paint and glue. You can find the instructions here <sup>4</sup>.
- You can make a **plastic bottle bird feeder** with a 2-liter bottle, some chopsticks, twine, a pin and birdseed. You can find the instructions here <sup>7</sup>.
- You can make **plastic bottle flowers** with empty water bottles, scissors, paint and pipe cleaners. You can find the instructions here <sup>3</sup>.

## Create a 3-course menu.



Sure, I can suggest a 3-course menu with a chocolate dessert for your vegetarian dinner party. Here are some possible options:

- Starter: **Wild Mushroom Tartlets with Onion Sauce** <sup>1</sup> or **Vegan Popcorn Tofu Nuggets** <sup>2</sup>
- Main: **Vegan Butternut Squash Mac** <sup>2</sup> or **Vegetarian Three-Bean Chili** <sup>3</sup>
- Dessert: **Chocolate Lava Cake** <sup>4</sup> or **Chocolate Pasta with Chocolate Hazelnut Cream Sauce, White Chocolate Shavings, and Fresh Berries** <sup>4</sup>

I hope this helps you plan your party. Enjoy! 😊

To read more: <https://www.microsoft.com/en-us/ai?rtc=1>

## *Number 20*

### NIST Selects ‘Lightweight Cryptography’ Algorithms to Protect Small Devices

The algorithms are designed to protect data created and transmitted by the Internet of Things and other small electronics.



Lightweight electronics, meet the heavyweight champion for protecting your information: Security experts at the National Institute of Standards and Technology (NIST) have announced a victor in their program to find a worthy defender of data generated by small devices. The winner, a group of cryptographic algorithms called **Ascon**, will be published as NIST’s lightweight cryptography standard later in 2023. You may visit: <https://csrc.nist.gov/projects/lightweight-cryptography>

#### Next Steps

NIST’s next steps will be to:

- Publish NIST IR 8454, which describes the details of the selection and the evaluation process
- Work with the Ascon designers to draft the new lightweight cryptography standard for public comments
- Host a virtual public workshop to further explain the selection process and to discuss various aspects of standardization (e.g., additional variants, functionalities, and parameter selections) as well as possible extensions to the scope of the lightweight cryptography project. The tentative dates for the workshop are June 21-22, 2023. More information will be provided in the upcoming weeks.

The chosen algorithms are designed to protect information created and transmitted by the Internet of Things (IoT), including its myriad tiny sensors and actuators.

They are also designed for other miniature technologies such as implanted medical devices, stress detectors inside roads and bridges, and keyless entry fobs for vehicles. Devices like these need “lightweight cryptography” — protection that uses the limited amount of electronic resources they possess.

According to NIST computer scientist Kerry McKay, the newly selected algorithms should be appropriate for most forms of tiny tech.

“The world is moving toward using small devices for lots of tasks ranging from sensing to identification to machine control, and because these small devices have limited resources, they need security that has a compact implementation,” she said. “These algorithms should cover most devices that have these sorts of resource constraints.”



To determine the strongest and most efficient lightweight algorithms, NIST held a development program that took several years, first communicating with industry and other organizations to understand their needs and then requesting potential solutions from the world's cryptography community in 2018.

After receiving 57 submissions, McKay and mathematician Meltem Sönmez Turan managed a multi-round public review process in which cryptographers examined and attempted to find weaknesses in the candidates, eventually whittling them down to 10 finalists before selecting the winner.

To read more: <https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices>

## Cyber Risk GmbH

Cyber Risk GmbH has been established in Horgen, Switzerland, by George Lekatis, a well-known expert in risk management and compliance.



### Online Training

Recorded on-demand training and live webinars.

[More »](#)



### In-house Training

Engaging training classes and workshops.

[More »](#)



### Social Engineering

Developing the human perimeter to deal with cyber threats.

[More »](#)



### For the Board

Short and comprehensive briefings for the board of directors.

[More »](#)



### Assessments

Open source intelligence (OSINT) reports and recommendations.

[More »](#)



### High Value Targets

They have the most skilled adversaries. We can help.

[More »](#)

## Cyber security training

### Overview

The world of cyber security and privacy is constantly changing. Today, effective cyber security programs involve the entire organization and not only the IT or the information security teams. Employees that have access to critical assets of an organization, have become primary targets of cyber attacks. Those that have access to technology and organizational assets are also responsible for the protection of those assets. Are they fit and proper to handle this responsibility? Do they have the awareness and skills necessary to meet these expectations?

Our training programs have the objective to help managers and employees not only understand the cyber security threats, but also their responsibility towards protecting the assets they handle. We explain how to proactively

apply good cyber security practices, how to identify threats and attacks, and what to do to protect themselves and their organizations. Cyber security is a shared responsibility.

## **Duration**

We tailor each program to the needs of each client. We can provide trainings as short as one hour, but we can also deep dive into our topics for one or two days. The duration depends entirely on the needs, the agreed content of the program, and the case studies.

## **Our Education Method**

In the core of our training approach is to ensure that our delivery is relatable, engaging, and interesting. We always make cyber security training an exciting adventure for our attendees. Our instructors have trained thousands of employees across the globe and have the skills and experience necessary to ensure that our attendees will enjoy the process while they learn. Our training programs may have workshop elements that get everyone involved.

## **Our Instructors**

They are working professionals that have the necessary knowledge and experience in the fields in which they teach. They can lead full-time, part-time, and short-form programs that are tailored to your needs. You will always know up front who the instructor of the training program will be.

## **Our websites include:**

### **a. Sectors and Industries.**

1. Cyber Risk GmbH - <https://www.cyber-risk-gmbh.com>
2. Social Engineering Training - <https://www.social-engineering-training.ch>
3. Healthcare Cybersecurity - <https://www.healthcare-cybersecurity.ch>
4. Airline Cybersecurity - <https://www.airline-cybersecurity.ch>
5. Railway Cybersecurity - <https://www.railway-cybersecurity.com>
6. Maritime Cybersecurity - <https://www.maritime-cybersecurity.com>
7. Oil Cybersecurity - <https://www.oil-cybersecurity.com>

8. Electricity Cybersecurity - <https://www.electricity-cybersecurity.com>
9. Gas Cybersecurity - <https://www.gas-cybersecurity.com>
10. Hydrogen Cybersecurity - <https://www.hydrogen-cybersecurity.com>
11. Transport Cybersecurity - <https://www.transport-cybersecurity.com>
12. Transport Cybersecurity Toolkit - <https://www.transport-cybersecurity-toolkit.com>
13. Hotel Cybersecurity - <https://www.hotel-cybersecurity.ch>
14. Sanctions Risk - <https://www.sanctions-risk.com>
15. Travel Security - <https://www.travel-security.ch>

## **b. Understanding Cybersecurity.**

1. What is Disinformation? - <https://www.disinformation.ch>
2. What is Steganography? - <https://www.steganography.ch>
3. What is Cyberbiosecurity? - <https://www.cyberbiosecurity.ch>
4. What is Synthetic Identity Fraud? - <https://www.synthetic-identity-fraud.com>
5. What is a Romance Scam? - <https://www.romance-scams.ch>
6. What is Cyber Espionage? - <https://www.cyber-espionage.ch>
7. What is Sexspionage? - <https://www.sexspionage.ch>

## **c. Understanding Cybersecurity in the European Union.**

1. The NIS 2 Directive - <https://www.nis-2-directive.com>
2. The European Cyber Resilience Act - <https://www.european-cyber-resilience-act.com>
3. The Digital Operational Resilience Act (DORA) - <https://www.digital-operational-resilience-act.com>

4. The Critical Entities Resilience Directive (CER) - <https://www.critical-entities-resilience-directive.com>
5. The Digital Services Act (DSA) - <https://www.eu-digital-services-act.com>
6. The Digital Markets Act (DMA) - <https://www.eu-digital-markets-act.com>
7. The European Health Data Space (EHDS) - <https://www.european-health-data-space.com>
8. The European Chips Act - <https://www.european-chips-act.com>
9. The European Data Act - <https://www.eu-data-act.com>
10. European Data Governance Act (DGA) - <https://www.european-data-governance-act.com>
11. The Artificial Intelligence Act - <https://www.artificial-intelligence-act.com>
12. The European ePrivacy Regulation - <https://www.european-eprivacy-regulation.com>
13. The European Cyber Defence Policy - <https://www.european-cyber-defence-policy.com>
14. The Strategic Compass of the European Union - <https://www.strategic-compass-european-union.com>
15. The EU Cyber Diplomacy Toolbox - <https://www.cyber-diplomacy-toolbox.com>

You may contact:

George Lekatis  
General Manager, Cyber Risk GmbH  
Dammstrasse 16, 8810 Horgen  
Phone: +41 79 505 89 60  
Email: [george.lekatis@cyber-risk-gmbh.com](mailto:george.lekatis@cyber-risk-gmbh.com)  
Web: [www.cyber-risk-gmbh.com](http://www.cyber-risk-gmbh.com)

## Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of interpretative;
- does not prejudice the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudice the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

*Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.*

General Terms and Conditions for all visitors to the Cyber Risk GmbH websites, and all legal transactions made through the Cyber Risk GmbH websites (hereinafter “GTC”):

<https://www.cyber-risk-gmbh.com/Impressum.html>

