January 2020, cyber risk and compliance in Switzerland
Top cyber risk and compliance related local news stories and world events

Dear readers,

Lucius Annaeus Seneca believed that *a kingdom founded on injustice never lasts*. Although the security risks are always very important, we have to respect privacy too, and we must ensure that security measures are proportional, fair and justified.

I have just read for the second time the new *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* (from the National Institute of Standards and Technology).

According to the new framework, *privacy risk management* is a cross - organizational set of processes that helps organizations understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks.

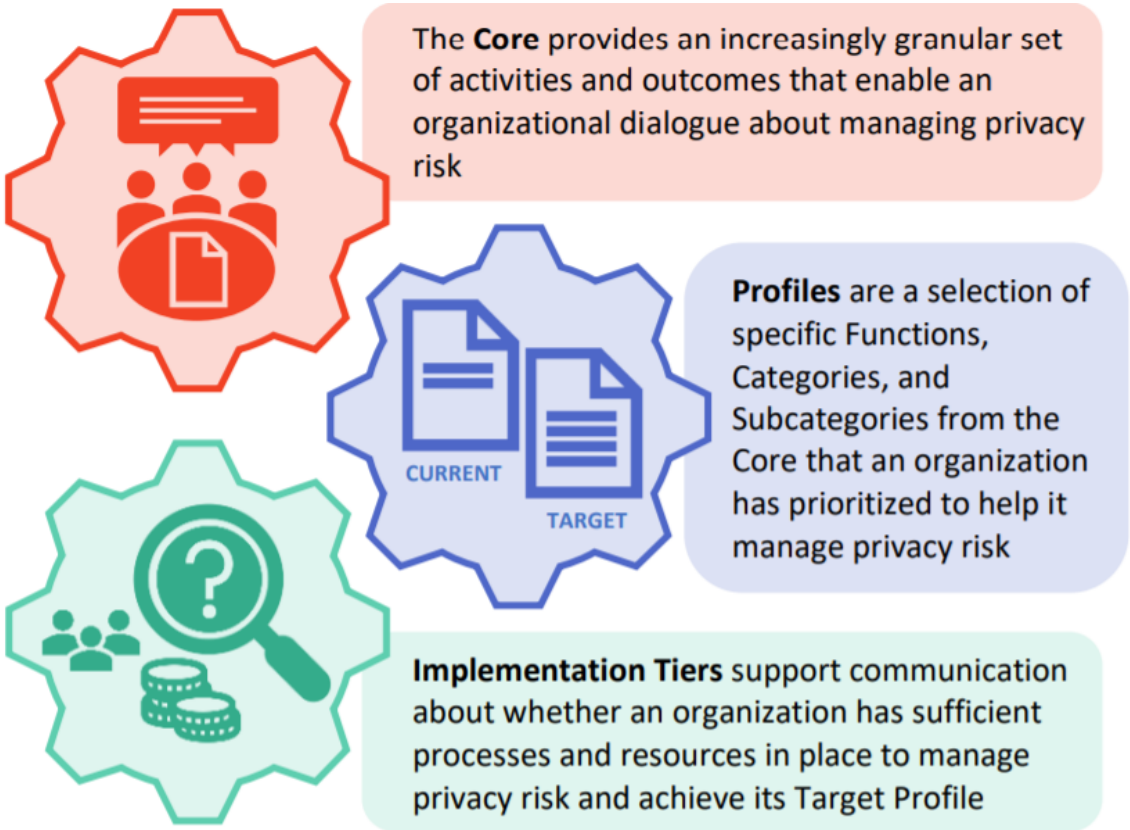
Privacy risk assessment is a sub-process for identifying and evaluating specific privacy risks. In general, privacy risk assessments produce the information that can help organizations to weigh the benefits of the data processing against the risks and to determine the *appropriate* response—sometimes referred to as proportionality.

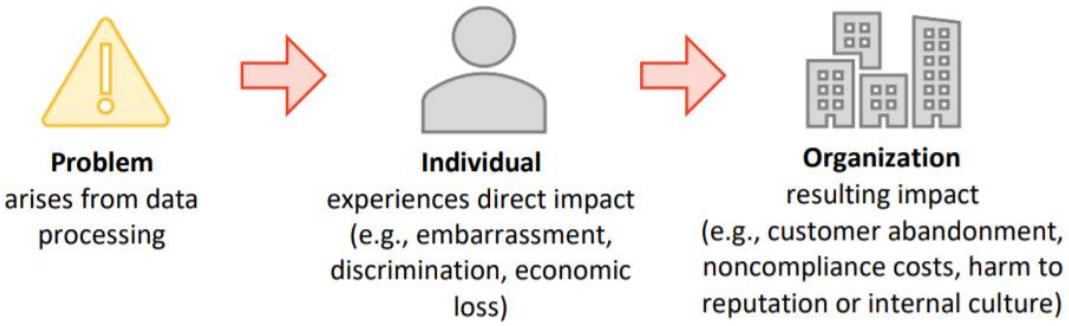
I like the structure of the privacy framework. It is composed of three parts: Core, Profiles, and Implementation Tiers.

The *Core* is a set of privacy protection activities and outcomes that allows for communicating prioritized privacy protection activities and outcomes across an organization from the executive level to the implementation / operations level.

A *Profile* represents an organization's current privacy activities or desired outcomes.

To develop a Profile, an organization can review all of the outcomes and activities in the Core to determine which are most important to focus on based on business or mission drivers, data processing ecosystem role(s), types of data processing, and individuals' privacy needs.





Implementation Tiers ("Tiers") provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk.

Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed.

When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk

management practices, the degree of integration of privacy risk into its enterprise risk management portfolio, its data processing ecosystem relationships, and its workforce composition and training program.

Read more at number 11 below.

The 18th of December 2019, the US Chairman of the Joint Chiefs of Staff General Mark A. Milley, met the Russian Chief of Staff General of the Army Valery Gerasimov, for bilateral talks in Berne.

The meeting was organized in the framework of the Good Offices of Switzerland on neutral ground, based on a request of both states and was facilitated by the Swiss Military Protocol.

In the aftermath, the designated Chief of the Swiss Armed Forces, Lieutenant General Thomas Süssli, met the two Generals separately for a brief exchange of views.

Welcome to our monthly newsletter.

Best regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Mobile: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com
Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Our catalog, *in-house* instructor-led training in Switzerland, Liechtenstein and Germany:
https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2020.pdf

Number 1 (Page 8)

USDOT Automated Vehicles Activities

The U.S. Department of Transportation (USDOT) and the White House Office of Science and Technology Policy invites public comment on the document, *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0 (AV 4.0).*

Number 2 (Page 10)

Expanded Transparency and More Controls for Political Ads

By Rob Leathern, Director of Product Management

Number 3 (Page 11)

EIOPA consults on guidelines on Information and Communication Technology security and governance

eiopa
European Insurance and Occupational Pensions Authority

Number 4 (Page 13)

European Commission publishes EU Cybersecurity Taxonomy

European Commission
JRC TECHNICAL REPORTS

A Proposal for a European Cybersecurity Taxonomy

Number 5 (Page 15)

Warnings about compromised passwords

Google Security Blog

Number 6 (Page 18)

Fake 'free giveaway' websites

National Cyber Security Centre

Number 7 (Page 19)

NIST Releases Data to Help Measure Accuracy of Biometric Identification

NIST National Institute of Standards and Technology U.S. Department of Commerce

Number 8 (Page 21)

Increased Geopolitical Tensions and Threats

Number 9 (Page 23)

Travelex New Year's Eve incident

National Cyber Security Centre

Number 10 (Page 25)

CRITICAL VULNERABILITY IN CITRIX APPLICATION

Number 11 (Page 26)

NIST Releases Version 1.0 of Privacy Framework

Tool will help optimize beneficial uses of data while protecting individual privacy.

National Institute of Standards and Technology
U.S. Department of Commerce

Number 12 (Page 29)

FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure

Number 13 (Page 31)

State of Vulnerabilities 2018/2019

enisa
European Network and Information Security Agency

Number 14 (Page 33)

Support for Windows 7 has ended

Microsoft

Number 1

USDOT Automated Vehicles Activities

The U.S. Department of Transportation (USDOT) and the White House Office of Science and Technology Policy invites public comment on the document, *Ensuring American Leadership in Automated Vehicle Technologies: Automated Vehicles 4.0 (AV 4.0).*

The United States Government is committed to fostering surface transportation innovations to ensure the United States leads the world in automated vehicle (AV) technology development and integration while prioritizing safety, security, and privacy and safeguarding the freedoms enjoyed by Americans.

1. Prioritize Safety

The U.S. Government will lead efforts to facilitate the safe integration of AV technologies, address potential safety risks, enhance the life-saving potential of AVs, and strengthen public confidence in these emerging technologies. The U.S. Government will also enforce existing laws to ensure entities do not make deceptive claims or mislead the public about the performance capabilities and limitations of AV technologies including, for example, deceptive claims relating to vehicle safety or performance.

2. Emphasize Security and Cybersecurity

The U.S. Government will support the design and implementation of secure AV technologies, the systems on which they rely, and the functions that they support to adequately safeguard against the threats to security and public safety posed by criminal or other malicious use of AVs and related services. The U.S. Government will work with developers, manufacturers, integrators, and service providers of AVs and AV services to ensure the successful prevention, mitigation, and investigation of crimes and security threats targeting or exploiting AVs, while safeguarding privacy, civil rights, and civil liberties. These efforts include the development and promotion of physical and cybersecurity standards and best practices across all data mediums and domains of the transportation system to deter, detect, protect, respond, and safely recover from known and evolving risks.

3. Ensure Privacy and Data Security

The U.S. Government will use a holistic, risk-based approach to protect the security of data and the public's privacy as AV technologies are designed and integrated. This will include protecting driver and passenger data as well as the data of passive third-parties—such as pedestrians about whom AVs may collect data—from privacy risks such as unauthorized access, collection, use, or sharing.

The U.S. Government recognizes the value of industry leadership in the research, development, and integration of AV innovations. Such innovation requires appropriate oversight by the Government to ensure safety, open markets, allocation of scarce public resources, and protection of the public interest.

Realizing the full potential of AVs will require collaboration and information sharing among stakeholders from industry, State, local, tribal, and territorial governments, academia, not-for-profit organizations, standards development organizations (SDO), and the Federal Government.

To read more:
https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf

Number 2

Expanded Transparency and More Controls for Political Ads

By Rob Leathern, Director of Product Management

New features will allow people to see fewer political and social issue ads on Facebook and Instagram.

We're updating our Ad Library to increase the level of transparency it provides for people and giving them more control over the ads they see.

The Ad Library is a unique tool to shine a light on political and social issue ads — a public archive that allows people to see all the ads politicians and campaigns are running on Facebook and Instagram and those that have run in the past.

This is an important step in making political ads more transparent and advertisers more accountable: the public can see every ad served to anyone in an easily searchable database.

We first launched the Ad Library in May 2018 and over the past several months we have spoken to dozens of political campaigns, activists, NGOs, nonprofits and volunteers about our policies for political ads.

Two themes we heard were that first, people want more transparency over who is using ads to try to influence voters and second, they want more control over the ads they see.

So today, we are announcing a number of updates to do just that.

To read more:
https://about.fb.com/news/2020/01/political-ads/

Number 3

EIOPA consults on guidelines on Information and Communication Technology security and governance

The European Insurance and Occupational Pension Authority (EIOPA) has launched a consultation on guidelines on Information and Communication Technology (ICT) security and governance.

These guidelines shall provide guidance to national supervisory authorities and market participants on how regulation regarding operational risks set forth in Directive 2009/138/EC and in the Commission's Delegated Regulation 2015/35 and EIOPA Guidance set out in EIOPA's Guidelines on System of Governance is applied in the case of ICT security and governance. The consultation is open until Friday, 13 March 2020.

In line with its Joint ESA's Advice and in reply to the European Commission's FinTech Action Plan, EIOPA developed these guidelines addressed to national supervisory authorities with the following objectives:

- To create a common baseline for information security throughout the EU Member States

- To enhance convergence of supervisory practices in this area

In developing the Joint Advice, the ESAs' objective was that every relevant entity should be subject to clear and general requirements on governance of ICT, including cybersecurity, to ensure the safe provision of regulated services.

As these requirements are not in general 'sector-specific for the (re)insurance market, EIOPA also considered the most recent guidelines published by the European Banking Authority

EIOPA's Guidelines cover the following areas:

- Governance and risk management
- ICT operations security
- ICT operations management

For responding to this consultation you may visit:
https://ec.europa.eu/eusurvey/runner/ICT_GLs

The deadline for submission of feedback is Friday, 13 March 2020 at 23.59 hrs CET.

Unless requested otherwise, all contributions received will be published after the deadline for submission.

To read more:
https://eiopa.europa.eu/Publications/Consultations/guidelines_ICT_security_and_governance_12122019_for_consultation.pdf

Number 4

European Commission publishes EU Cybersecurity Taxonomy

On 12 September 2018, the Commission has proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (COM/2018/630).

The overall mission of the Competence Centre and the Network (CCCN) is to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market.

This goes hand-in-hand with the key objective to increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other European industries.

One of the first steps during the Impact Assessment of the Proposed Regulation was to provide a clear definition of the cybersecurity context, its domains of application, research and knowledge.

In this context, the first version of the proposed taxonomy was published with the goal of aligning the cybersecurity terminologies, definitions and domains.

The taxonomy was then used for the categorisation and mapping of existing EU cybersecurity centres (e.g. research organisations, laboratories, associations, academic institutions, groups, operational centres, etc.) according to their cybersecurity expertise in specific domains.

Based on this first analysis, a survey was also conducted where more than 600 institutions participated and registered their cybersecurity expertise.

In order to assess essential aspects of the CCCN regulation proposal, the Commission launched a pilot phase under Horizon 2020. In particular, the proposals CONCORDIA, ECHO, SPARTA and CyberSec Europe were selected as the four pilot projects to assist the EU in the establishment of a European Cybersecurity Competence Network of cybersecurity centres of excellence.

The pilots bring together more than 160 partners, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

The four pilot projects were asked to review the proposed taxonomy and provided feedback, which was used to improve the first version of the taxonomy in order to publish this second enhanced version.

For the purpose of this document, cybersecurity is considered an interdisciplinary domain. This starting point finds support in the Cybersecurity Report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism in March 2017, where it is stated clearly that:

"cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments and the pace of technical change and innovation. In short, cybersecurity is much more than a science".

To read more:
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

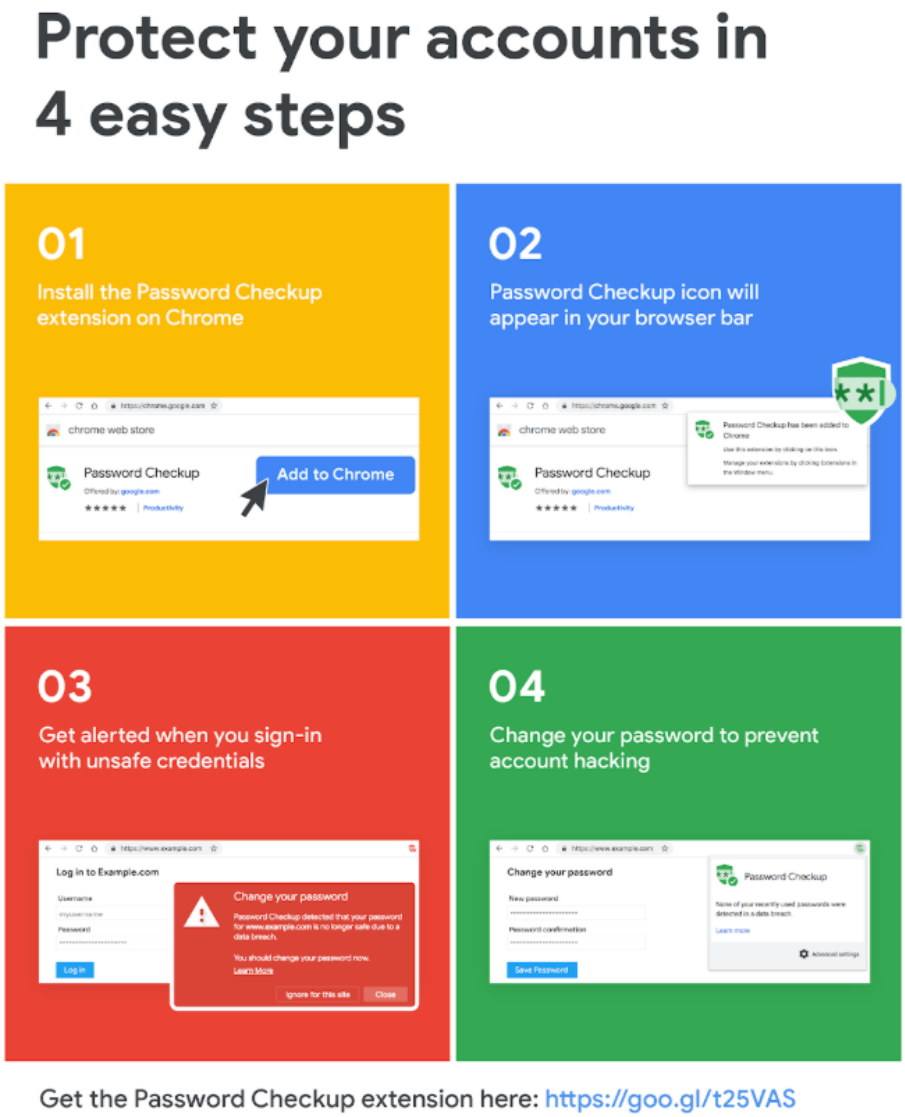
Number 5

Warnings about compromised passwords

Google Security Blog

Google first introduced password breach warnings as a Password Checkup extension early this year. (You may visit: https://chrome.google.com/webstore/detail/password-checkup-extensio/pncabnpcffmalkkjpajodfhijclecjno?hl=en)

It compares passwords and usernames against over 4 billion credentials that Google knows to have been compromised. You can read more about it at: https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html



In October, Google built the Password Checkup feature into the Google Account, making it available from passwords.google.com.

Chrome's integration is a natural next step to ensure we protect even more users as they browse the web.

Here is how it works:

- Whenever Google discovers a username and password exposed by another company's data breach, we store a hashed and encrypted copy of the data on our servers with a secret key known only to Google.

- When you sign into a website, Chrome will send a hashed copy of your username and password to Google encrypted with a secret key only known to Chrome.

  No one, including Google, is able to derive your username or password from this encrypted copy.

- In order to determine if your username and password appears in any breach, we use a technique called private set intersection with blinding that involves multiple layers of encryption.

  This allows us to compare your encrypted username and password with all of the encrypted breached usernames and passwords, without revealing your username and password, or revealing any information about any other users' usernames and passwords.

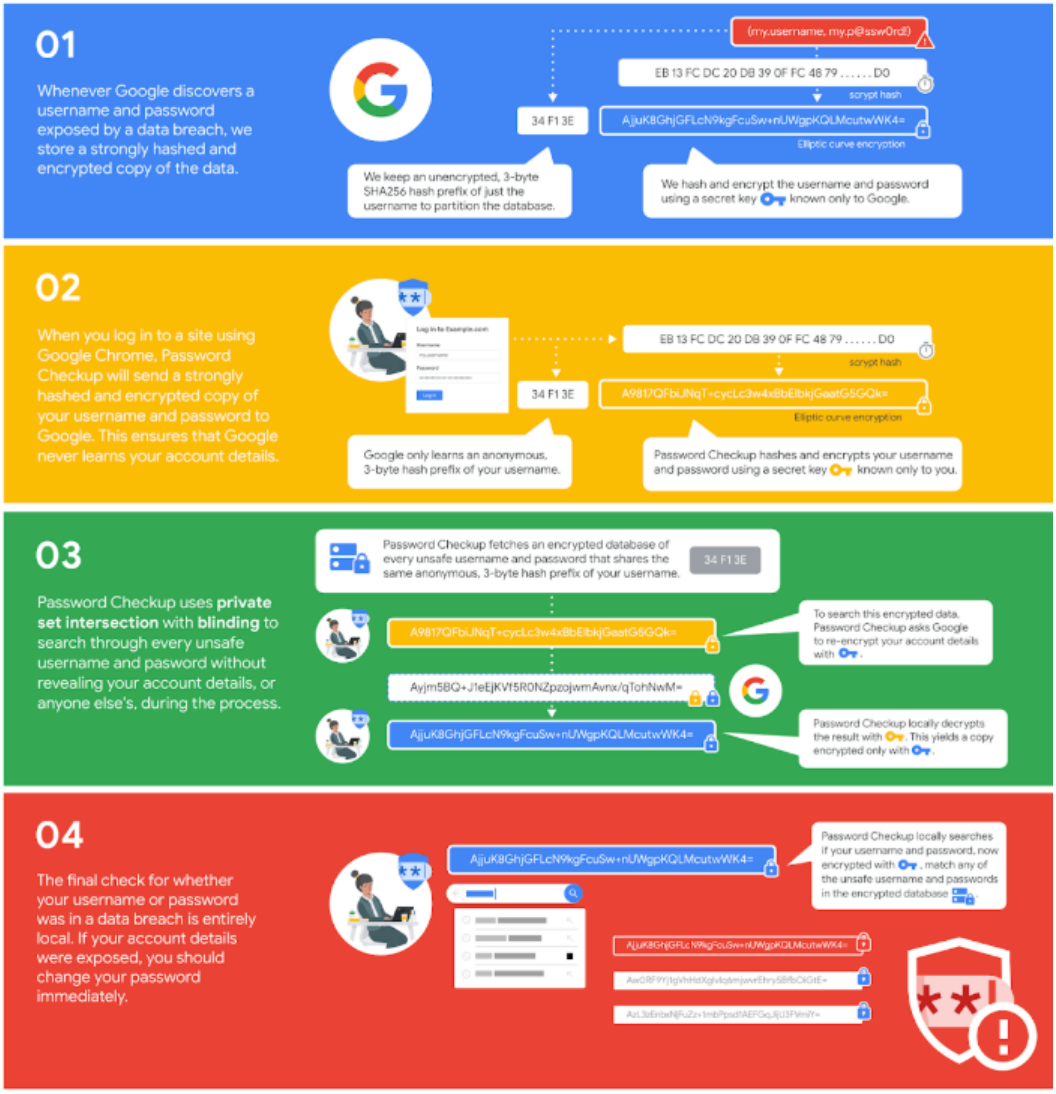
  In order to make this computation more efficient, Chrome sends a 3-byte SHA256 hash prefix of your username to reduce the scale of the data joined from 4 billion records down to 250 records, while still ensuring your username remains anonymous.

- Only you discover if your username and password have been compromised.

  If they have been compromised, Chrome will tell you, and we strongly encourage you to change your password.

Under the hood:

How Password Checkup for Google Chrome helps keep your accounts safe



Number 6

Fake 'free giveaway' websites

Cyber security researchers have uncovered a fake 'free giveaway' website that tricks users into revealing their login credentials.

Cyber criminals posted links to a phishing website in the comments section of the legitimate Steam website, encouraging users to visit a convincing – but fake – page that contained free downloadable content for the platform.

In order to download the content, users were instructed to log in to the fake site using their Steam credentials. While the screen looks like a legitimate Steam login page, any usernames and passwords that users entered were sent to the attackers instead.

Phishing scams such as this are a particularly devious method used by cyber criminals to steal sensitive information, and it can be a worrying time for victims.

The NCSC has produced guidance for spotting and dealing with phishing emails. You may visit:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Number 7

NIST Releases Data to Help Measure Accuracy of Biometric Identification

National Institute of Standards and Technology
U.S. Department of Commerce

New biometric research data — ranging from fingerprints to facial photographs and iris scans — is now available from the National Institute of Standards and Technology (NIST).

Stripped of identifying information and created expressly for research purposes, the data is designed primarily for testing systems that verify a person's identity before granting access — be it to another room or another country.

Few available resources exist to help developers evaluate the performance of the software algorithms that form the heart of these systems, and the NIST data will help fill that gap.

"This all gets back to reproducible research," said NIST computer scientist Greg Fiumara. "The data will help anyone who is interested in testing the error rates of biometric identification systems."

The files, which are available on the NIST website, are organized into three Special Databases (SDs).

Numbered SD 300, SD 301 and SD 302, they represent the first in what is intended to be an expanding collection of biometric resources. You may visit: https://www.nist.gov/itl/iad/image-group/resources/biometric-special-databases-and-software

While the three databases contain varied types of data collected at different times, two of them contain information gathered during the Nail to Nail Fingerprint Challenge, an IARPA-funded competition that NIST helped to design and carry out.

One of the new resources, SD 301, is significant for being the first "multimodal" dataset NIST has ever released.

Multimodal means that an individual's different biometric markers — in this case face, fingerprints and iris scan — are all linked so that they can be used together for identification by systems that use a combination of identification approaches, such as a photograph from the individual's face in addition to their fingerprints.

“This opens up possibilities for types of multimodal research that haven’t been done before,” Fiumara said. “We want to get more secure and more accurate identification, as multimodal systems are harder to spoof.”

SD 302 contains fingerprint data from a few hundred people gathered by a mixture of eight commercially available and prototype devices.

Data collected during both portions of the Nail to Nail challenge includes prints taken with contactless fingerprint devices, a technology that could simplify and speed up print gathering as it improves.

“It also includes latent fingerprint data, in which prints are left while handling everyday objects,” Fiumara said. “Realistically and expertly collected latent data is difficult to come by.”

All of the individuals represented in the two sets have formally consented to the inclusion of their biometric and demographic data and its distribution for use in advancing research, Fiumara said. The data has been scrubbed of identifying information such as their names and places of residence.

Rounding out the datasets is SD 300, a collection of fingerprints taken from 900 old ink cards. All of the record cards have been stripped of identifying data and are from individuals who are now deceased.

According to Fiumara, a benefit of the data is helping manufacturers evaluate how well their modern systems can produce results that will be interoperable with hard-copy ink records, which will remain important to the criminal justice system for some time.

As a whole, the group of three SDs contain data retained with archival-grade lossless compression — a step forward, Fiumara said, because the research data sets in the past often did not retain this level of fidelity to the original image.

Each dataset in the series has an accompanying user’s guide offering background about collection methods and other details useful to researchers.

Number 8

Increased Geopolitical Tensions and Threats

Increased geopolitical tensions and threats of aggression may result in cyber and physical attacks against the Homeland and also destructive hybrid attacks by proxies against U.S. targets and interests abroad.

Knowing how you, your organization, and your personnel may be exposed or targeted during increased tensions can help you better prepare.

In many cases, implementing the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials can dramatically improve your defenses.

Should an incident occur, engage with partners, like CISA, and work with cyber or physical first responders to gain technical assistance. Review your organization from an outside perspective and ask the tough questions—are you attractive to Iran and its proxies because of your business model, who your customers and competitors are, or what you stand for?

To read more:
https://www.cisa.gov/sites/default/files/publications/CISA-Insights-Increased-Geopolitical-Tensions-and-Threats-S508C.pdf

The Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials: https://www.cisa.gov/cyber-essentials

CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

Consistent with the NIST Cybersecurity Framework and other standards, the Cyber Essentials are the starting point to cyber readiness. Reducing an organization's cyber risk requires a holistic approach, similar to that taken to address other operational risks.

Yourself +

Your Staff +

Your Systems +

Your Surroundings +

Your Data +

Your Actions Under Stress +

Booting Up: Things to Do First +

Number 9

Travelex New Year's Eve incident

National Cyber Security Centre

There has been prominent media coverage this week after foreign exchange company Travelex suffered a ransomware attack on New Year's Eve.

The company has taken all of its systems offline in a move they said will prevent the spread of the virus further across the network. Travelex have said there had been no evidence customer data had been compromised.

Travelex worldwide money

We're sorry but our online travel money service isn't available right now.

This is as a result of a software virus. On discovering the virus, and as a precautionary measure, Travelex immediately took all its systems offline to prevent the spread of the virus further across the network.

Whilst the investigation is still ongoing, to date our investigation shows that customer data has not been compromised.

We have now contained the virus and are working to restore our systems and resume normal operations as quickly as possible.

Travelex's network of branches continue to provide foreign exchange services manually and a number of workarounds are provided below.

We apologise to our customers for any inconvenience caused as a result.

Travelex is in discussions with the Metropolitan Police who are conducting their own criminal investigation.

You can still visit us in-store:

Our travel money stores are open 7 days a week. To find your nearest store, please contact our Customer Service team on 0345 872 7627 or via social media.

Have a Travelex Money Card?

We are currently unable to sell or reload travel cards online. Existing cards continue to work as normal for spending and ATM withdrawals.

If you bought your card in the UK, you can view your balance and transaction information at uk.travelexmoneycard.com and reload by calling the number on the back of your card.

Have a query about an existing online order?

For customers who have ordered money online, please contact Travelex Customer Services on 0345 872 7627 or via social media.

Please note: Travelex will never e-mail you to request your personal information, payment card or bank account details. If you get a call you are not expecting and or you are unsure about the identity of a caller you should end the call and call back using the telephone number on the Travelex website.

Media reports have said those responsible for the attack have set a ransom to the company, and have threatened to release data obtained through the attack. The Information Commissioner's Office (ICO) have been in contact with Travelex to advise on "potential personal data issues".

The NCSC has guidance for organisations looking to defend against the threat of ransomware. Guidance such as mitigating malware is also of use with this kind of cyber attack.
You may visit: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

Limiting the impact of a ransomware attack

The following measures can all help to limit the impact of a ransomware attack.

- Good **access control** is important. The compartmentalisation of user privileges can limit the extent of the encryption to just the data owned by the affected user. Understand the risks brought in by the system administration model that your IT architecture uses. Re-evaluate permissions on shared network drives regularly to prevent the spreading of ransomware to mapped and unmapped drives. System administrators with high levels of access should avoid using their admin accounts for email and web browsing.
- Ransomware doesn't have to go viral in your organisation; limit access to your data and file systems to those with a business need to use them. This is good practice anyway and, like many of the recommendations we make here, prevents against a range of cyber attacks.

Number 10

CRITICAL VULNERABILITY IN CITRIX APPLICATION

On December 17, 2019, Citrix® published an advisory for a critical vulnerability (CVE-2019-19781) in Citrix Application Delivery Controller (Citrix ADC™/NetScaler ADC™) and Citrix Gateway™ (NetScaler Gateway™).

If unmitigated, adversaries could exploit this vulnerability to gain remote code execution on affected appliances without credentials, potentially enabling access to other internal resources and sensitive data.

Citrix also released an interim mitigation for the vulnerability. Citrix Virtual Apps and Desktops™ users typically access their applications and desktops through Citrix ADC or Citrix Gateway appliances that are frequently deployed in front of Citrix Virtual Desktop Infrastructure (VDI) products and web applications.

The appliances are often accessible from the Internet to allow remote connections, increasing their risk of exploitation.

Security researchers have reproduced an exploit for this vulnerability and have detected scanning for vulnerable appliances and exploitation attempts in the wild.

To read more: https://media.defense.gov/2020/Jan/10/2002233132/-1/-1/0/CSA%20FOR%20CITRIXADCANDCITRIXGATEWAY_20200109.PDF

Number II

NIST Releases Version 1.0 of Privacy Framework

Tool will help optimize beneficial uses of data while protecting individual privacy.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

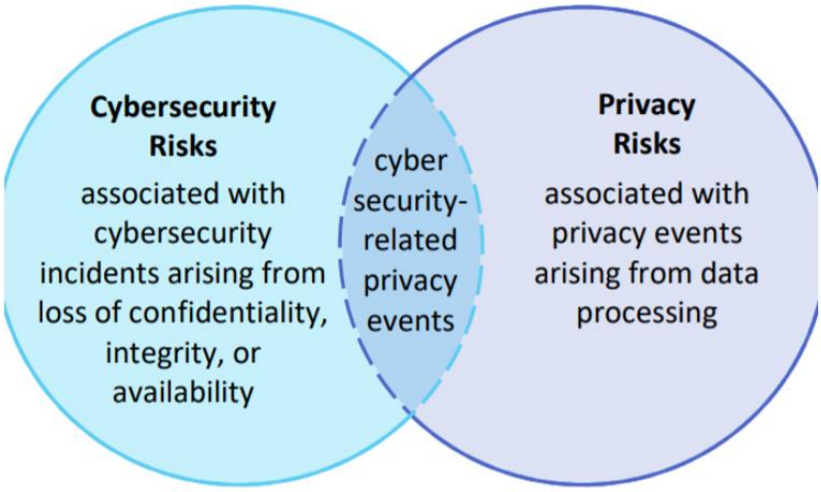
Our data-driven society has a tricky balancing act to perform: building innovative products and services that use personal data while still protecting people's privacy.

To help organizations keep this balance, the National Institute of Standards and Technology (NIST) is offering a new tool for managing privacy risk.

The agency has just released Version 1.0 of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.

Developed from a draft version in collaboration with a range of stakeholders, the framework provides a useful set of privacy protection strategies for organizations that wish to improve their approach to using and protecting personal data.

The publication also provides clarification about privacy risk management concepts and the relationship between the Privacy Framework and NIST's Cybersecurity Framework.



"Privacy is more important than ever in today's digital age," said Under Secretary of Commerce for Standards and Technology and NIST Director Walter G. Copan. "The strong support the Privacy Framework's development has already received demonstrates the critical need for tools

to help organizations build products and services providing real value, while protecting people's privacy."

Personal data includes information about specific individuals, such as their addresses or Social Security numbers, that a company might gather and use in the normal course of business.

Because this data can be used to identify the people who provide it, an organization must frequently take action to ensure it is not misused in a way that could embarrass, endanger or compromise the customers.

The NIST Privacy Framework is not a law or regulation, but rather a voluntary tool that can help organizations manage privacy risk arising from their products and services, as well as demonstrate compliance with laws that may affect them, such as the California Consumer Privacy Act and the European Union's General Data Protection Regulation. It helps organizations identify the privacy outcomes they want to achieve and then prioritize the actions needed to do so.

"What you'll find in the framework are building blocks that can help you achieve your privacy goals, which may include laws your organization needs to follow," said Naomi Lefkovitz, a senior privacy policy adviser at NIST and leader of the framework effort. "If you want to consider how to increase customer trust through more privacy-protective products or services, the framework can help you do that. But we designed it to be agnostic to any law, so it can assist you no matter what your goals are."

Privacy as a basic right in the USA has roots in the U.S. Constitution, but its application in the digital age is still evolving, in part because technology itself is changing at a rapidly accelerating pace.

New uses for data pop up regularly, especially in the context of the internet of things and artificial intelligence, which together promise to gather and analyze patterns in the real world that previously have gone unrecognized. With these opportunities come new risks.

"A class of personal data that we consider to be of low value today may have a whole new use in a couple of years," Lefkovitz said, "or you might have two classes of data that are not sensitive on their own, but if you put them together they suddenly may become sensitive as a unit.

That's why you need a framework for privacy risk management, not just a checklist of tasks: You need an approach that allows you to continually reevaluate and adjust to new risks."

The Privacy Framework 1.0 has an overarching structure modeled on that of the widely used NIST Cybersecurity Framework, and the two frameworks are designed to be complementary and also updated over time.

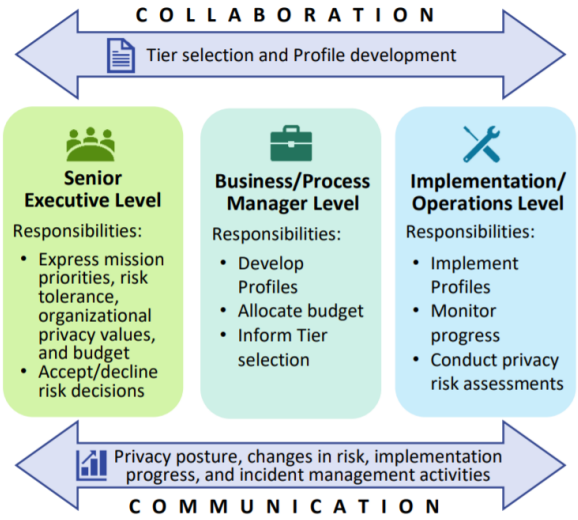
Privacy and security are related but distinct concepts, Lefkovitz said, and merely adopting a good security posture does not necessarily mean that an organization is addressing all its privacy needs.

As with its draft version, the Privacy Framework centers on three sections: the Core, which offers a set of privacy protection activities; the Profiles, which help determine which of the activities in the Core an organization should pursue to reach its goals most effectively, and the Implementation Tiers, which help optimize the resources dedicated to managing privacy risk.

The NIST authors plan to continue building on their work to benefit the framework's users. Digital privacy risk management is a comparatively new concept, and Lefkovitz said they received many requests for clarification about the nature of privacy risk, as well as for additional supporting resources.

"People continue to yearn for more guidance on how to do privacy risk management," she said. "We have released a companion roadmap for the framework to point the way toward more research to address current privacy challenges, and we are building a repository of guidance resources to support implementation of the framework. We hope the community of users will contribute to it to advance privacy for the good of all."

To read more:
https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf



Number 12

FBI Announces New Policy for Notifying State and Local Election Officials of Cyber Intrusions Affecting Election Infrastructure

The Federal Bureau of Investigation (FBI) announced a new internal policy to clarify and guide the timely federal notification of appropriate state and local officials of cyber intrusions affecting election infrastructure.

Protecting the integrity of elections in the United States against criminal activity and national security threats is among the top priorities of the Department of Justice (DOJ) and the FBI.

Cyber intrusions affecting election infrastructure have the potential to cause significant negative impacts on the integrity of elections.

Understanding that mitigation of such incidents often hinges on timely notification, the FBI has established a new internal policy outlining how the FBI will notify state and local officials responsible for administering election infrastructure of cyber activity targeting their infrastructure.

The FBI's new policy recognizes the necessity of notifying responsible state and local officials of credible cyber threats to election infrastructure.

Each state has a designated person to serve as its chief state election official with ultimate authority over elections held in the state, which often includes certifying election results.

However, most election infrastructure is owned and operated by local governments.

Likewise, the local election process is overseen by local election officials. The FBI's interactions regarding election security matters must respect both state and local authorities.

Thus, the FBI's new policy mandates the notification of a chief state election official and local election officials of cyber threats to local election infrastructure.

The new policy is informed by existing FBI policies surrounding cyber incident notification thresholds and cyber victim notification in general.

The new policy, however, provides updated and additional guidance on the timely dissemination of notifications and/or threat reporting; the protection of victim information and disclosures; and coordination between FBI and other agencies in regard to election security for maximum impact.

Decisions surrounding notification continue to be dependent on the nature and breadth of an incident and the nature of the infrastructure impacted.

It is the intent of the FBI that this new policy will result in increased collaboration between all levels of government for the integrity and security of U.S. elections.

Number 13

State of Vulnerabilities 2018/2019

The vulnerability ecosystem has matured considerably in the last few years. A significant amount of effort has been invested to systematically capture, curate, taxonomize and communicate the vulnerabilities in terms of severity, impact and complexity of the associated exploit or attack.

Standardisation in the description of vulnerabilities contributes not only to effective threat intelligence sharing, but also potentially efficient threat management, provided that organisations, vendors and security researchers actively seek to discover the vulnerabilities and respond in a timely fashion.

As the standardisation of cataloguing and modelling the vulnerabilities reaches the aforementioned maturity, public or private (i.e. commercial) databases containing information of the actual vulnerabilities (and some with their exploits counterparts) have emerged.

As there are a number of initiatives within the research community, quite naturally some databases could be considered to be more “authoritative” and/or “reliable” than others.

However, due to the nature of the vulnerability ecosystem, it is not a reasonable assumption that the databases will be complete (that is, contain all vulnerabilities), or reliable in the sense that the information captured is correct, in the sense that the samples gathered can be considered to reliably help in drawing conclusions on the whole population.

This is influenced by a number of factors, including the quality of analysis and assessment, the assessment framework itself, the economic aspects (such as the value of any available exploit), as well as the business models of the software vendors, threat intelligence services, and the overall security community.

The purpose of this report is to provide an insight on both the opportunities and limitations the vulnerability ecosystem offers. By using the vulnerabilities published during the year of 2018 and Q1-Q2 of 2019 as a vehicle, this report goes beyond the standard exploratory analysis,

which is well captured by many industry whitepapers and reports, and attempts to answer questions related to the reliability, accuracy of the vulnerability sources and the widely accepted evaluation metrics.

The report: https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/

Number 14

Support for Windows 7 has ended

Microsoft

After 10 years, support for Windows 7 ended on 14 January 2020. We know change can be difficult, so we are here to help you with recommendations for what to do next and to answer questions about end of support.

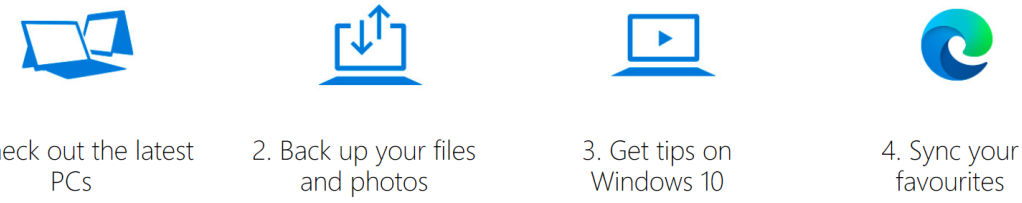
As of 14 January 2020, your computer running Windows 7 will still function but Microsoft will no longer provide the following:

- Technical support for any issues
- Software updates
- Security updates or fixes

While you could continue to use your PC running Windows 7, without continued software and security updates, it will be at greater risk for viruses and malware.

Going forward, the best way for you to stay secure is on Windows 10. And the best way to experience Windows 10 is on a new PC. While it is possible to install Windows 10 on your older device, it is not recommended.

More information at: https://www.microsoft.com/en-gb/windows/windows-7-end-of-life-support-information



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 prejudge 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 prejudge 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.