SECTRA NEWSLETTER – December 2024

Monthly Review

Cybersecurity news from around the world

ARTICLE

Finland implements a new cybersecurity plan

Read article →

SECTRA

General cybersecurity news

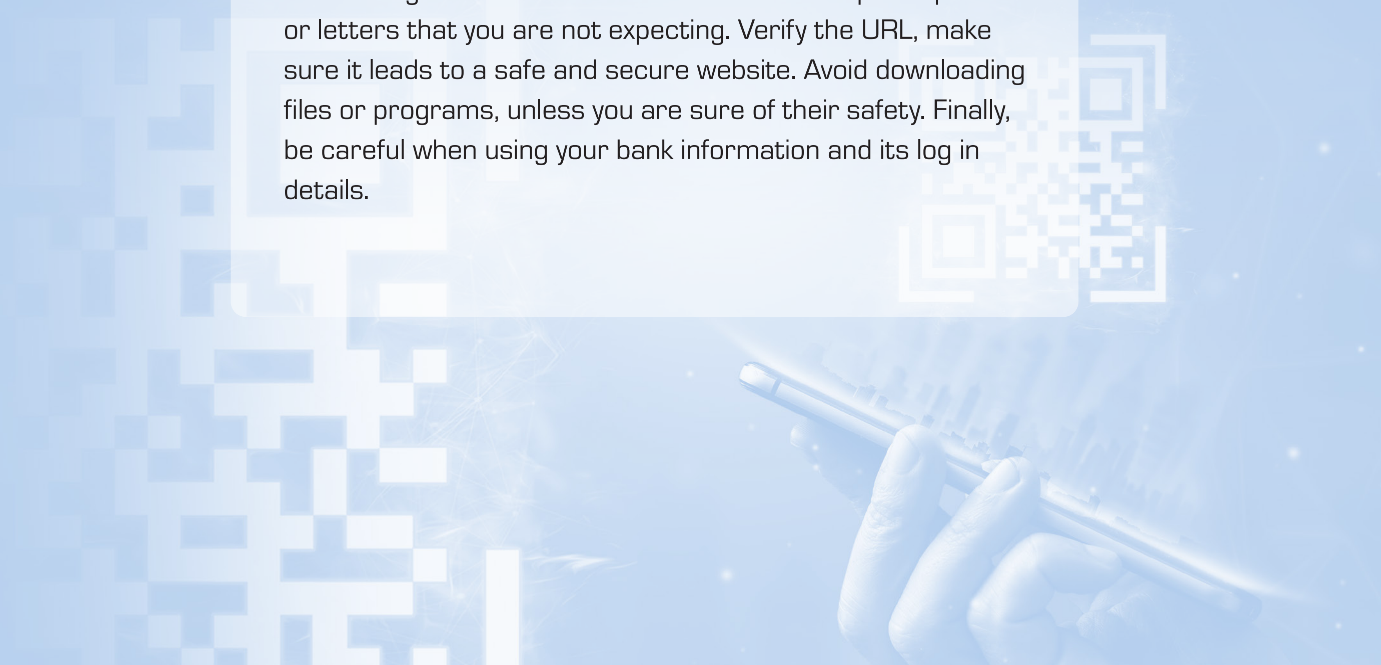
1

Cybercrime — from online to paper

Criminals that use QR codes or "Quishing" to lure users into downloading hurtful codes or data, is not a new phenomenon — but a new report shows that it has taken a turn.

In November the local Swiss cybersecurity authority announced that letters had been sent out by criminals saying it was from the local Swiss meteorological institute. In the letter they advertised a new weather app that easily could be downloaded using the QR code. But instead of an app, the users downloaded a malware called Coper and Octo2, that aims to steal sensitive data from the user, like log in credentials for their mobile banks.

The Swiss cybersecurity authorities explained that the malware was made for Android mobile devices — but that there is no information about the number of victims. The dangers with QR codes become clear when taking the Swiss-event in regard. However, there are precautions to take when using QR codes. Be careful with codes in public places or letters that you are not expecting. Verify the URL, make sure it leads to a safe and secure website. Avoid downloading files or programs, unless you are sure of their safety. Finally, be careful when using your bank information and its log in details.



2 Navigating risks in international relations

China’s cyber espionage is a known threat, highlighted by a U.S. incident where Chinese hackers accessed telecom networks like T-Mobile, AT&T, and Verizon, stealing call logs, unencrypted texts, and even listening to phone calls. China’s focus is on gathering intelligence, not disruption. Swedish businesses in critical infrastructure and high-tech industries must be vigilant against these risks.

Despite suspicions around companies like Huawei and TikTok, no direct evidence of espionage has been proven. However, due to China's laws requiring cooperation with intelligence services, caution is necessary. Given China's importance in global supply chains, avoiding collaboration is challenging, and Sweden’s "value-based realism" suggests ongoing dialogue with China while managing cybersecurity risks.

3 The majority use AI – but few have an approved policy in place

AI technology is rapidly expanding, particularly within the Swedish financial sector. However, efforts to manage the associated risks often lag behind. A recent report from the Swedish Financial Supervisory Authority “*AI allt vanligare i finanssektorn men riskhanteringen släpar efter*”, shows that only 41 percent of Swedish financial firms have policies for using AI tools (such as ChatGPT, Copilot, and Gemini), despite 84 percent of the 234 surveyed companies using these tools for various tasks.

The EU’s Artificial Intelligence Regulation, effective from August 2024, applies to all sectors, including finance, with most provisions enforced starting in 2026. The regulation aims to classify AI systems by risk, banning those that pose unacceptable risks and allowing high-risk systems if they meet certain requirements. Of companies using AI (in finance), 91 percent have either started preparing for the AI Regulation’s implementation or plan to do so in the coming months.

ARTICLE

Authority exploitation: A new cybercriminal tactic

Cyberattacks pose a growing threat to organizations, with significant financial and reputational risks. The magnitude of sanctions from authorities when a breach is discovered can cost millions.

Sanctions for data breaches can differ depending on the location of the company or organization. Within the EU, companies may face penalties up to €20 million or 4% of their total turnover from the previous financial year, whichever is higher, if a breach is discovered. In contrast, the United States has different regulations, with each state enforcing its own rules regarding data breaches. For example, just over a month ago, the New York Attorney's Office required an auto insurance company to pay a €9.28 million fine and a travel insurance company a €1.47 million fine for violations of New York's SHIELD Act — intended to strengthen the Information Security Breach and Notification Act. These breaches involved cybercriminals obtaining sensitive personal data of their customers. →

In recent years, cybersecurity laws have become stricter regarding how organizations handle sensitive information. If a data breach occurs, the company is to blame and must ensure it has proper security to protect personal data. For modern companies, data is crucial, and a breach can lead to heavy fines, reputational damage, and loss of customers.

> *"Each data breach that occurs globally, costs on average €4.6 millions."*

More frequent and sophisticated cyberattacks

The rising number and growing sophistication of cyberattacks is an increasing concern. They are not only more frequent but also more advanced. In the latest report from IBM, regarding the cost of a data breach, the numbers show that the cost is the highest it has ever been. Each data breach that occurs globally, costs on average €4.6 million — and seen from last year, there has been an increase of as much as ten percent.

Cybercriminals have begun using a method known as Ransomware-as-a-Service, with actors like RansomedVC. Rather than reporting a data breach to authorities, they extort victims for an amount smaller than the potential fine. They can vary between €50,000 up to €200,000 depending on the size of the company. Some who have been exposed to the method by RansomedVC include the tech giant Sony, the US capital Washington D.C. Election Commission and Japan's largest telecom operator NTT Docomo.

Even so, it is a fact that a cyberattack results in high costs and loss of trust for the affected company. That said, companies can take proactive steps to reduce the risks of a breach and its potential consequences. →

Five essential steps to enhance cybersecurity
Although the cyber attacks are more and more advanced, the simple methods should not be underestimated.

1. **Strong and complex passwords:** Enforce a company-wide policy requiring passwords to be at least 12 characters, include a mix of letters, numbers, and symbols, and mandate regular changes.
2. **Prevent use of personal devices**: They lack proper security measures and pose a risk of data breaches, malware, and exposure to unsecured networks.
3. **Use VPN to encrypt data:** Protect sensitive information, especially for remote employees connecting to company networks over unsecured networks.
4. **Regularly delete nonessential data:** Reduce the risk of breaches. However, ensure compliance with legal regulations, as some data must be retained for specific periods.
5. **Implement endpoint protection**: To secure devices like phones, computers, and IoT devices from malware and cyberattacks, as they are common entry points for data breaches.

Strengthen your defense and safeguard your information:
Companies and organizations must take proactive measures to protect their data from rising cyber threats. Although cyberattacks are on the rise, organizations can fight back by boosting cybersecurity with strong passwords, VPNs, smart data management, and endpoint protection. Making their defenses stronger and more reliable than ever. ■

ARTICLE

Finland implements a new cybersecurity plan – on all levels

In agreement with the NIS2 Directive, more and more EU countries are drawing up implementation plans for increased cybersecurity. In Finland, a strategy has now been developed for all levels of society.

The NIS2 Directive is the EU-wide legislation governing cybersecurity, aiming to ensure a high and uniform level of cybersecurity across all member states of the Union. In December, Finland released a strategy outlining how organizations and companies can implement the new cybersecurity measures in their operations. The implementation plan is designed to provide practical steps that support the overall cybersecurity strategy, helping to achieve its goals across the society. The plan has been prepared under the leadership of the Director of National Cyber Security in collaboration with public and private sector representatives, the scientific community, and non-governmental organizations.

The plan outlines the necessary measures to be taken, including financing, scheduling, and responsibility allocation. It also provides a detailed description of the monitoring and information processes, which will be managed by the cyber security strategy monitoring group. →

The information collected will be processed by the Director of Cyber Security, who will compile a follow-up report for submission to political decision-makers and relevant authorities, offering a comprehensive overview of the strategy's implementation.

Higher requirements in NIS2 Directive

The EU's decision on NIS2, made in December 2022, establishes clearer security requirements and risk assessment protocols compared to the previous 2018 legislation. The directives also expand to cover additional sectors, necessitating the inclusion of more supervisory authorities.

In Sweden, an investigation is currently underway to determine how these new directives will be implemented. However, due to the lack of definitive answers regarding the regulations, the process is expected to conclude by spring 2025.

> *"Concerns have been raised regarding the number of measures proposed and their practical implementation."*

The directives target operators within 18 critical sectors, including drinking water, transportation, and healthcare. Their goal is to ensure that businesses establish and implement a comprehensive information security system in a systematic manner.

Concerns regarding the Finnish implementation plan

While the Finnish implementation plan has seen success in several areas, concerns have been raised regarding the number of measures proposed and their practical implementation. →

Specific concerns include the timeframe, which spans several political mandates, and uncertainties regarding the financing of these measures. Although it is stated that funding should come from additional resources, these resources have yet to be allocated. Despite these concerns, the plan is viewed positively from a cybersecurity perspective, and Finland sees it as a step in the right direction for improving its cybersecurity strategy.

What to expect from the Swedish investigation

In Sweden, we can expect a detailed investigation to adapt and implement the NIS2 cybersecurity directives. The directive covers more sectors and introduces clearer requirements for security measures and risk assessments, which will require careful adaptation to Sweden's specific context.

This investigation will offer guidelines for Swedish businesses on how to comply with the directives, including identifying affected sectors and specifying the necessary security measures. However, precise regulations on implementation and financing in Sweden are expected to be clarified by spring 2025.

Ultimately, this process will strengthen Sweden's cybersecurity framework, improve coordination across sectors, and foster a broader understanding of cybersecurity's importance, thereby ensuring greater resilience and trust in the face of emerging digital threats. ■

Key takeaways

1. Criminals in Switzerland are using fake QR codes in letters to spread malware that steals sensitive data, prompting warnings about the risks of scanning unverified QR codes.

2. China's cyber espionage threat highlights the need for Swedish businesses to stay vigilant while balancing cybersecurity risks with essential international collaborations.

3. AI is widely used in Sweden's financial sector, but most firms lack risk management policies as they prepare for the EU's 2024 AI regulation.

4. Cybercriminals extort their victims with penalty payments from authorities. Threating with the amount of fines from authorities is a new form of extortion by cybercriminals.

5. The implementation plan for Finland's national cybersecurity strategy was published in December.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden,
and operates through offices in Sweden, the Netherlands and Finland.