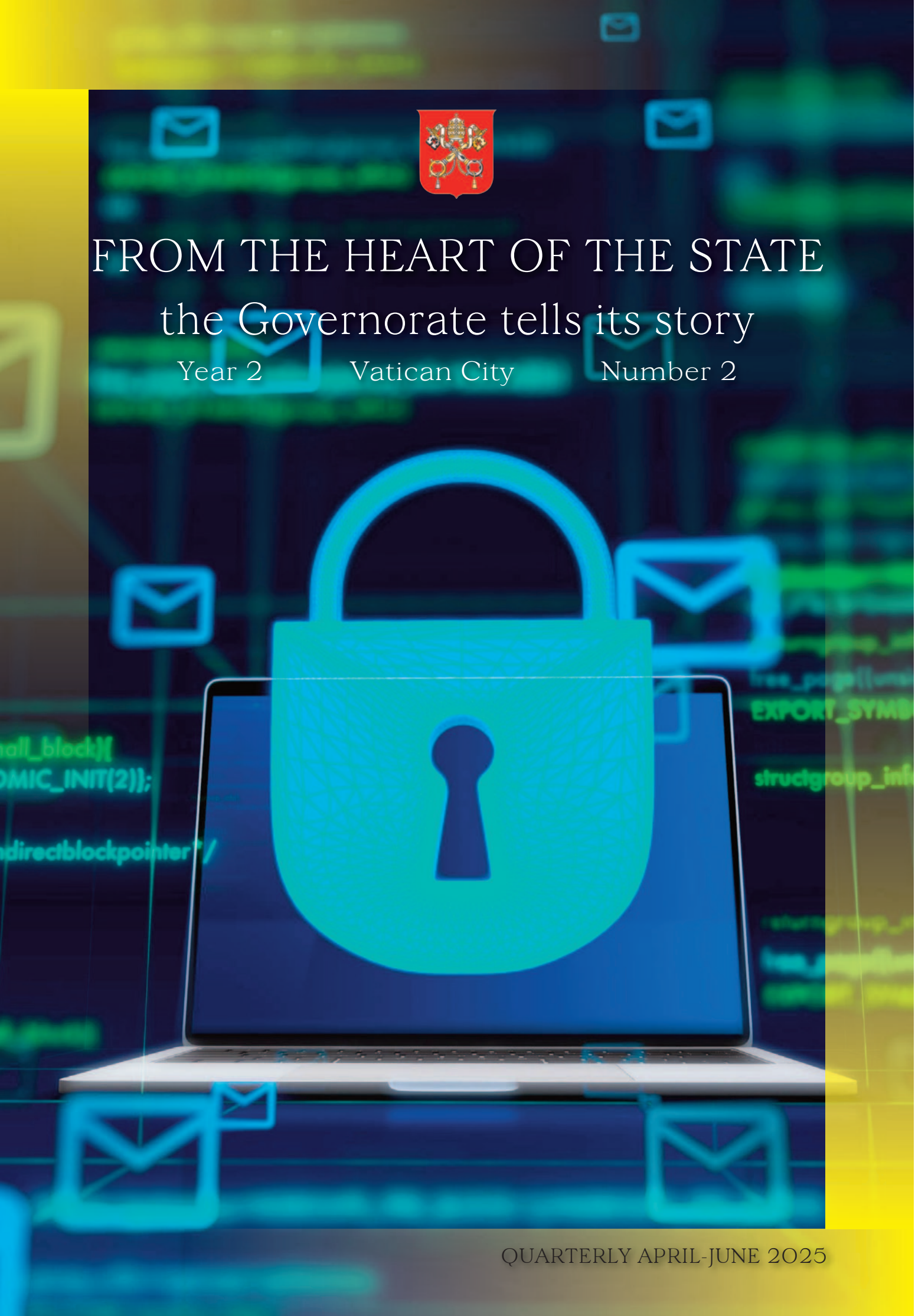
FROM THE HEART OF THE STATE

the Governorate tells its story

Year 2 Vatican City Number 2



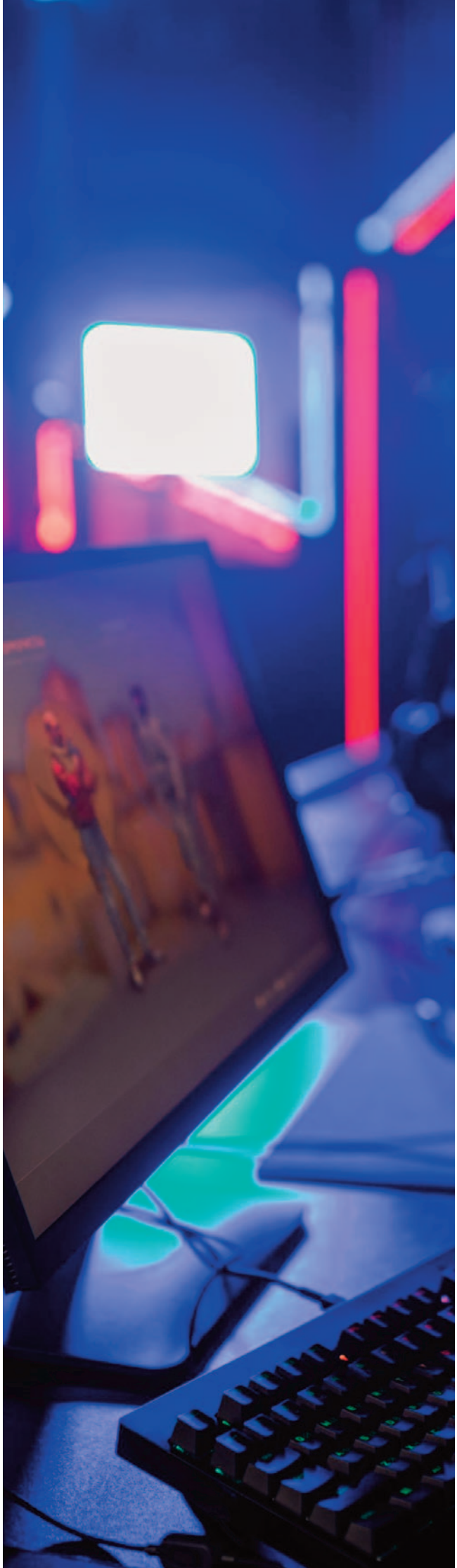
QUARTERLY APRIL-JUNE 2025

Published by the Governorate of Vatican City State
Institutional Communication
00120 Vatican City

Email: comunicazione@scv.va
Website: www.vaticanstate.va

X (Twitter): Governatorato_scv
Instagram: Governatorato_scv

Editor: Nicola Gori
Publisher: Governatorato dello Stato della Città del Vaticano



CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

The decision to dedicate this newsletter to cybersecurity is to offer a simple guide to help navigate and protect oneself in a complex and multifaceted reality. We firmly believe that - on a personal level - everyone shares a part of the responsibility to maintain its integrity.

Given their implications, issues related to cybersecurity go far beyond technical aspects. They involve, among other things, several dimensions: risk management, law, communication, privacy, economics, and more.

It is clear that cybersecurity is a highly specialized field, involving experts in computer science, mathematics, or physics. However, it has now become a part of our daily lives, just like the digital world and, more recently, artificial intelligence. Cybersecurity focuses on protecting computer systems, networks, data, and devices from cyber threats, attacks, and privacy breaches. Its goal is to ensure the confidentiality and availability of digital resources, to prevent damage and guarantee protection and safety in all digital activities.

In this context, it is essential to be aware that within the Vatican Governorate, where IT tools are used, everyone shares a degree of responsibility in protecting the institution.

In this newsletter, you will find some useful tips recommended by a group of industry experts for managing our daily interactions with the cyber world. Among the most important suggestions are being particularly cautious with unexpected requests,

email attachments, and potentially inactive USB devices. In case of doubt, it is always best to seek advice and inform the IT security officer.

Cyberattacks can indeed have very negative effects on the integrity of digital infrastructures. Cybercriminals often seek financial gain, such as in the case of ransomware attacks. However, they also aim to obtain confidential information that can impact individuals—such as stolen personal data (i.e. identity theft), which is then sold to criminal organizations for their own nefarious purposes.Moreover, an attack on an institutional entity can also damage public trust. When a website is attacked, the institution's reputation is inevitably affected.

In some cases, compromising the integrity of IT systems can even disrupt the very functioning of the organization. Attacks can be especially devastating when the target is a hospital system or a transportation service.

It is essential to be informed and aware of one's personal responsibility to prevent giving malicious actors an opportunity to hack one's IT system, therefore, this newsletter wishes to offer some particularly valuable and practical advice to help work with confidence.

Nicola Gori

SECURITY AS TOP PRIORITY

The Governorate of the Vatican City State has always placed the security and protection of its IT systems first. This commitment has characterized the birth and development of the Internet network within the Vatican State and its operating systems.

The resources allocated to cybersecurity are signifcant because they aim to primarily protect and safeguard the image of the Pope and the daily use of devices by the State for his service.

For this purpose, on 18 July 2024, the Directorate of Security and Civil Protection Services of the Governorate signed a Memorandum of Understanding with the Agency for National Cybersecurity of the Italian Republic (ACN).

The goal is to facilitate the exchange of information, training activities and cybersecurity projects that increase technical and scientific skills and capabilities in the field of risk prevention related to crime in cyberspace. This was an important step to ensuring greater cooperation in the development of training programs in the field of cybersecurity.

With emphasis on the exchange of information, experiences and procedures in this sector, it aims to safeguard cyberspace while also promoting research projects to enhance technical and scientific capabilities and skills.

It is clear that this Memorandum of Understanding is only one part of the Governorate's effort to ensure the cornerstones of cybersecurity for all its entities: perimeter defense, information security, identity and access management (IAM), data integrity and availability.

Despite the significant investment in cybersecurity, proper operating systems and technology alone are not enough. The collaboration of every member of the Governorate's working community is essential. This human factor is what makes the difference and ensures a heightened level of protection.

Therefore, this newsletter aims to present an opportunity to learn and adopt best practices that can prevent possible criminal infiltration.

With this intention, I wish you an insightful read.

Sr. Raffaella Petrini

President of the Governorate of the Vatican City State

CYBER SECURITY: A STRATEGIC VISION BETWEEN TECHNOLOGY, RESILIENCE AND SECURITY CULTURE

In an increasingly interconnected world where digitalization permeates every area, cyber security is no longer a technical issue limited to IT Services but represents one of the main strategic challenges for the protection of services, data and assets. Cyber threats, with their ability to strike quickly on a large scale and with transversal impacts, increasingly require a systemic and continuous response.

In the current context, we are called upon to develop a long-term strategic vision for the protection of our digital space. This vision must be based on three fundamental pillars:

- secure infrastructures and processes,
- advanced technical skills;
- a widespread security culture.

The analysis of the current situation shows that digital infrastructures – networks, data centers, platforms – are now structured to guarantee robustness, operational continuity and reliability, even in consideration of cost containment. However, the rapid evolution of technologies and the exponential increase in threats require a model of continuous evolution. It is not just about updating hardware and software, but about transforming the entire system into an adaptive and intelligent infrastructure, capable of interpreting data and reacting in real time. In this sense, the adoption of zero trust architecture models, system virtualization and the integration of artificial intelligence in detection mechanisms represent key elements for an advanced defense.

Traditionally, cyber security has focused on perimeter protection: firewalls, antivirus, network segmentation. Today, this approach is no longer sufficient. Attacks are not limited to forcing the "entrance doors" but exploiting internal vulnerabilities, human behavior and connected devices.

A modern cyber security strategy must therefore include:

- Continuous monitoring and threat intelligence: the ability to analyze data flows in real time, identify anomalous patterns and anticipate malicious behavior.

- Incident response and operational resilience: prepare structured incident response plans and ensure business continuity even during attacks.
- Cyber deterrence: strengthening defensive capabilities to discourage attackers, including through international cooperation and cyber diplomacy.
- End-to-end protection: ensuring security at every stage of the data lifecycle, from collection to storage, up to destruction.

This approach implies a transition from simple defense to proactivity: identifying, evaluating and neutralizing threats before they turn into incidents.

One of the most underestimated, yet decisive, aspects of cyber security is the oft-cited human factor. Statistics confirm that a significant percentage of cyber attacks are due to human errors, carelessness or lack of awareness. For this reason, alongside technological innovation, it is essential to promote a culture of security that involves every level of the organization, from top decision makers to end users. In this context, initiatives such as continuous training programs for all staff, awareness campaigns

on phishing and social engineering, attack simulations and cyber hygiene courses as fundamental tools for creating a safe ecosystem.

For example, you can enhance the following five factors of cyber hygiene in your work structure:

• Segmentation. The data network should be segmented into limited areas that guarantee the protection of the entire system and eliminate the vulnerability of access points to attacks. This type of security also tends to satisfy the protection even in the case of remote working needs. If there were to be a breach, the intrinsic security will be able to contain it without compromising the rest of the activities.

• Encryption. If firewalls and access protocols are breached and other defenses fail, encryption ensures that all the critical data that has been stored is effectively useless once in the hands of cyber criminals. If you don't know how to decode and put it back together, encrypted data becomes a difficult puzzle to solve. Good cyber hygiene presupposes encrypting files and data before sharing them. The same goes for encrypting network traffic, where possible.

• Two-factor authentication. Security is increasingly linked to the person - facial recognition and fingerprints are an example.

Even just implementing basic two-factor authentication can be helpful in stopping a first wave of breaches. The more personal authentication becomes, the more secure networks will be. After all, it is much more complicated to steal a thumbprint rather than a PIN code!

• Constant updating. Malware is evolving and becoming more sophisticated and it is necessary to be ready apply the updates which are regularly released for this purpose.

• Minimal privilege. Even if you have full trust in your employees, it does not mean that everyone actually needs the same levels of access. A good method of working safely is to grant the employee's user account only the access that they actually need. By minimizing access to sensitive data, you limit the points of vulnerability.

Finally, looking to the future, beyond the concept of cyber security in itself, equally important is the broader and more ambitious factor of cyber resilience. This means:

• predicting the unpredictable,
• responding flexibly and quickly to critical events,
• restoring functions within certain time frames,
• adapting and constantly improving.

In cyberspace, resilience is more important than invulnerability. Maximum protection is achieved by investing in the construction of a strong cyber identity based on resilient infrastructures, conscientious people and a multi-level strategic action plan. Only in this way will it be possible to face the present digital security challenges and those in the future.

Ing. Antonino Intersimone
Director of the Directorate for Telecommunications and Information Systems

10 GOLDEN RULES FOR ONLINE SAFETY: HOW TO PROTECT YOUR DIGITAL LIFE FROM THREATS AND FRAUD

Online safety is one of the chief concerns of the digital era. Protecting one's data and identity online is crucial in order to avoid fraud, identity theft and cyberattacks. Below are 10 essential rules to browse safely and reduce risks.

1. Use strong and unique passwords and opt for passphrases

According to the guidelines of the **National Institute of Standards and Technology (NIST)**, strong passwords contain at least **12-16 characters**, including **upper and lower case letters**, **numbers** and **special characters**, and avoid commonly used words. NIST guidelines recommend using a **password manager** to generate and store credentials safely, and avoiding the use of the same password for multiple accounts.

In cybersecurity, the use of passphrases is highly recommended. Unlike traditional passwords, passphrases are a sequence of words aimed at ensuring a greater amount of protection in authentication processes.

Whereas conventional passwords are often limited to a maximum of 16 characters, passphrases can contain 100 or more characters. Their structure is based on a combination of words, punctuation and upper and lower case letters, making them extremely resistant to cyberattacks, and easy for users to recall.

Passphrases strengthen security against unauthorized access and improve usability. Unlike the complex sequence of letters and numbers of traditional passwords, passphrases are based on phrases that make sense and are more intuitive and more difficult to forget.

This type of authentication is now widely used in contexts that require high security standards, such as the cryptography of data and protection of operating systems and advanced applications. The fact that many digital platforms recommend passphrases highlights the need for changes to protection policies regarding

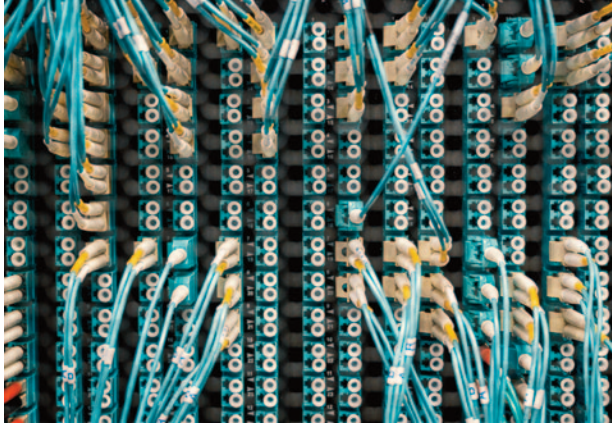
digital access, and emphasizes the importance of a balance between security and usability.

2. Enable Multifactor Authentication (MFA)

Multifactor authentication (MFA) adds a further level of security by requiring multiple methods of authentication to access accounts. In addition to a password, this may include OTP codes sent via SMS or authentication apps, biometric authentication and hardware security keys, making unauthorized access more difficult. **NIST recommends** the use of **authentications apps** or **physical security keys** rather than SMS messages, which can be intercepted.

3. Be cautious of suspicious emails and messages (phishing)

Phishing aims to extract sensitive information by mimicking official communication. It is important not to click on suspicious links and to always verify the source of a message before providing personal data or bank details. According to the **National Centre for Cybersecurity (NSCS)**, more than **90% of cyberattacks** begin with a phishing email.



4. Regularly update devices and software

System and application updates often contain **security corrections** to protect devices from known vulnerabilities. Implementing automatic updates is an excellent practice. NIST and other security organizations recommend immediately implementing security patches to avoid attacks from known exploits.

5. Protect sensitive information and privacy

Avoid sharing personal or financial information on websites that are not secure and limit the data published on social media. It is advisable to review privacy settings to check who can see your content. The **General Data Protection Regulation** (GDPR) underscores the importance of protecting personal data to prevent any misuse.

6. Verify the security of websites

Before inputting sensitive data into a website, make sure to use the **HTTPS** protocol and that the SSL certificate is valid. Reliable websites have a lock icon next to the address on the browser. According to the **Google Transparency Report**, websites that do not use HTTPS are more vulnerable to man-in-the-middle interceptions and attacks.

7. Avoid using unprotected public Wi-Fi networks

Public Wi-Fi connections are often vulnerable to cyberattacks. If they must be used, it is recommended to only visit safe websites and to use a **VPN (Virtual Private Network)** to protect the data being transmitted. The **Federal Bureau of Investigation (FBI)** recommends not accessing bank accounts or sensitive data on unprotected public Wi-Fi networks.

8. Be cautious with attachments and downloads

Files and program uploads from unreliable sources can contain malware. It is a good practice to verify the source of the file before opening it and to use updated **antivirus software**. According to the **Cybersecurity and Infrastructure Security Agency (CISA)**, attachments in exe, .zip and .js formats are the most common vehicles for malware.

9. Regularly check your accounts

Monitor the activity of your online accounts for any suspicious access. Services like **"Have I been Pwned"** allow users to check if their credentials have been compromised and their data violated. The **NCSC** recommends activating notifications for unrecognized access and immediately changing passwords in cases of suspected violations.

10. Use reliable security tools

The use of **updated antivirus software**, an **active firewall** and a **VPN** will help protect data from malware and unauthorized access. It is important to choose security tools that are reliable and produced by trusted companies. The **NIST** recommends users to always enable the security functions integrated in operating systems, such as firewalls and access verification.

Conclusion

Following these 10 rules will **reduce the risk of cyberattacks** and keep digital identities safe. Being aware of the risks and being prudent are the best ways to protect oneself from online threats. The implementation of these practices provides a good protection from digital threats.

Emmanuele Valeri

RANSOMWARE: THE LAST FRONTIER IN DIGITAL EXTORTION AND HOW TO PROTECT YOURSELF

You turn on your computer one morning and find a disturbing message on your screen:
"Your files have been encrypted. In order to have them back, pay a ransom in cryptocurrency within 72 hours!"
This dramatic scenario is a reality faced by many businesses and users on a daily basis, due to ransomware: one of the most devastating threats of cybersecurity.

What is ransomware?
Ransomware (ransom from ancient French, ranson, meaning ransom and ware an abbreviation for software) is a type of malware aimed at blocking access to data through cryptography. The attackers request a ransom, usually in the form of cryptocurrency like Bitcoin or Ethereum, in exchange for the decryption key needed to recover files.
There are two main types of ransomware:
• **Locker ransomware:** blocks access to the device making it unusable
• **Crypto Ransomware:** encrypts specific files, such as documents, images and databases, leaving the operating system working, in order to allow communication with the attackers
Ransomware attacks spread in various ways. The following are some of them.
• **Phishing emails:** The attackers send email messages that appear to be from reliable sources. The emails contain malicious links or attachments, which when opened, install the ransomware on the victim's device.
• **Downloads from compromised websites:** Visiting websites that are not secure or downloading software from unreliable sources can expose users to hidden malware.
• **Vulnerabilities in systems:** Hackers take advantage of security flaws in software or operating systems to introduce ransomware. This is particularly common when updates and patches are not used.
• **Infected USB devices:** Physical devices such as USB keys can also be used to spread ransomware.
• **Targeted attacks:** Large businesses are often the victims of targeted attacks in which the attackers study their network and look for its weak points before striking.

Why is ransomware so dangerous?
Ransomware is dangerous for several reasons:
• **Loss of data:** Without adequate backups, the encrypted data could potentially not be recovered.
• **Financial impact:** The payment of the ransom, the cost of recovery and the resulting downtime can lead to significant financial costs.
• **Damages to reputation:** A ransomware attack can undermine the trust of clients and business partners.
• **Constant evolution:** Ransomware is increasingly more sophisticated, making it more difficult for companies to protect themselves.

How to protect oneself from Ransomware?

Prevention is the key to protection from this threat. The following are some effective strategies to reduce the risk of a ransomware attack:

• **Regular backups:** Save data regularly on external devices or secure cloud services. Ensure that backups are isolated from the main network to avoid them from being affected by cyberattacks

• **Updates and Patches:** Always update operating systems and software. Ransomware takes advantage of known flaws that can be resolved with promptly applied patches.

• **Training employees:** It is fundamental for businesses to educate their employees to recognize suspicious emails and other social engineering techniques. Regular training can prevent human error.

• **Advanced security solutions:** Use antivirus software, firewalls and systems to identify intrusions to monitor and block any suspicious activity. Many tools also include specific protection against ransomware.

• **2 Factor Authentication (2FA):** Protect accounts with two forms of identification to make it more difficult for hackers to access company systems.

• **Limited Access:** Implement the principle of minimum privilege, allowing employees to access only the resources they need for their work. This limits potential damages in case of an attack.

• **Monitoring and Periodic Audits:** For businesses, regularly checking the security of their systems can help identify vulnerabilities that could be exploited.

• **Strategies to respond to attacks:** Prepare a detailed plan on how to respond in the event of a ransomware attack. It should include instructions on how to isolate affected systems, communicate with the interested parties and begin the recovery of data.

What to do in case of an attack?

In case of a ransomware attack, it is crucial to take prompt action:

• **Isolate affected systems:** Immediately disconnect the affected devices from the network to prevent the malware from spreading.

• **Never pay the ransom!!!:** Paying the ransom does not guarantee the recovery of data and contributes to financing further attacks.

• **Contact the authorities:** Report the incident to law enforcement or other competent authorities.

• **Consult with cybersecurity experts:** Experts in the sector can help mitigate damages and find solutions to restore systems (for example: https://www.nomoreransom.org).

Conclusion

Ransomware is one of the threats that has the greatest impact in the digital era. However, with the right precautions, it is possible to drastically reduce the risk of being attacked. Investing in employee cybersecurity training, in technologies and in hiring experts specialized in cybersecurity are essential steps in protecting businesses and people. Cybersecurity should not be seen as a luxury, but rather as a fundamental need in an ever more connected world.

CYBERSECURITY AND SMART HOMES: THE SECURITY OF CONNECTED DEVICES AND NEW THREATS TO PRIVACY

Introduction
The growing spread of technology in people's homes has radically changed the way in which we interact with our domestic environment. With household appliances connected to advanced security systems, the concept of "smart home" has made our homes more efficient and comfortable. However, the integration of these devices introduces new cybersecurity and privacy problems that cannot be ignored.

Vulnerability of IoT devices
One of the main risks has to do with the vulnerabilities of IoT devices (Internet of things). Unlike computers and smartphones that are often equipped with strong security measures, many smart household devices are equipped with minimal protection standards. This makes them easy targets for hackers, who can access surveillance cameras, thermostats and voice assistants to compromise the security of the home and the privacy of users. Once a device has been violated, an attacker could use it to monitor domestic activities, access sensitive information or even take control of other devices connected to the network.

Users' lack of awareness
Another important aspect is user awareness with regards to cybersecurity. Many consumers purchase smart devices without knowing the risks associated with them. They often do not change default credentials or do not update their software regularly, leaving themselves open to hacker access. This failure of attention to basic measures increases the risk of violations and intrusions. Moreover, users rarely monitor their domestic network traffic, which makes it difficult to identify potential anomalies or suspicious activity.

Personal Data Protection
In addition to direct attacks to devices, there is an increasing concern for the protection of personal data. Smart devices gather a large amount of information on users, including daily habits and biometric data. If this information ends up in the wrong hands, it can be used for identity theft, unauthorized surveillance or even the setting up of detailed profiles for advertising aims. Some producers have policies that are not entirely transparent with regards to data management, which makes it difficult for users to know how and where data is stored.

Large scale cyberattacks
Cyber threats are not limited to individual users and can have large scale consequences. Cybercriminals can exploit IoT devices to create botnets, networks of devices that have been infected that are used to make largescale attacks, such as the Distributed Denial of Service (DDoS). One example of this is the 2016 Mirai botnet attack, which exploited thousands of vulnerable IoT devices to block entire online services. This demonstrates how an adequate management of cybersecurity in homes can have repercussions also on a global scale.

Solutions and responsibilities
Facing these challenges requires the joint effort of producers, users and institutions. Producers should adopt better security standards, implement advanced cryptography and provide automatic software updates to correct any potential vulnerabilities. Users should adopt basic security practices, such as changing their default passwords, implementing 2 Factor Authentication and regularly monitoring their connected devices.

The role of regulations
With regards to regulation, some steps forward have been made, with regulation that imposes the minimum standards of security for IoT devices. With the GDPR, the European Union has emphasized data protection, but the rapid evolution of technology demands constant updates to regulation to guarantee adequate security. It is crucial that businesses be held accountable for the protection of user data and that strict measures be implemented to prevent potential violations.

Conclusion
In a time in which technology is increasingly more present in our lives, guaranteeing the security of connected devices should be a priority. Smart homes offer many advantages in terms of automation and comfort, but without adequate protection, the risk of compromise is high. Only through an attentive approach and the implementation of advanced security measures will it be possible to take full advantage of the benefits of technology, without compromising privacy and digital security.

SOCIAL ENGINEERING: HOW CRIMINALS EXPLOIT HUMANS TO PENETRATE SYSTEMS

On a typical day at work, you receive an urgent call from a person who identifies himself as a member of the IT department. Very politely and kindly, he informs you that a critical problem with your account requires the confirmation of some personal information, and that providing the password and the authentication code, will resolve the security issue without any loss of time. The reassuring and mild tone of the conversation could lead you to trust and cooperate, but it is precisely in situations like these that cybercriminals strike. This is a classic example of social engineering.

What is Social Engineering?

Social engineering is the manipulation of people to obtain access to protected information or systems. Instead of trying to compromise complex cybersecurity systems, criminals focus on non-technological targets: human beings. Cybercriminals exploit victims' trust, fear and curiosity and create an urgency to induce them to make damaging actions such as clicking on a suspicious link, download an infected file or reveal reserved credentials.

Some of the most common forms of social engineering

1. Phishing

Phishing is probably the most widespread social engineering technique. It occurs via emails, messages or phone calls (vishing: voice phishing) that appear to come from reliable sources. Criminals try to trick victims into providing sensitive information or downloading malware.

2. Pretexting

Attackers uses a pretext, a credible story, to earn their victim's trust. For example, they may pretend to be a human resources employee or a supplier of services.

3. Baiting

Baiting relies on people's curiosity. A classic example is using a USB key left intentionally in a public pace, perhaps with an attractive label such as "company salaries". Once the device is connected to a computer, the malware infects the system.

4. Tailgating

This technique takes place in the physical world. A criminal infiltrates a protected building by following someone who has access or pretending to have forgotten their badge.

Why is social engineering so effective?

The success of social engineering is based on some psychological factors:

- **Trust:** People tend to trust individuals who appear to be professional or have authority.
- **Urgency:** Time pressure often leads victims to make impulsive decisions.
- **Emotions:** Fear or curiosity can make people take action without thinking.

How can one protect oneself?

Protection from social engineering requires a combination of factors, including good habits and security tools. The following are practical recommendations for the workplace:

1. Ongoing training

Awareness is the first step. Participating in regular training

courses on cybersecurity can make the difference. These should not be complex lessons. Even simple sessions that update employees on how to recognize social engineering techniques can help. Moreover, periodically simulating attacks (such as fake phishing attempts) can test the preparation of employees.

2. Strict policies of verification
Never provide sensitive information to anyone who initiates contact without warning, even if their request seems legitimate. Before taking any action, it is advisable to take a moment to verify the identity of the person. For example, if an "IT employee" asks for a password, it may be useful to call the IT department directly, using an official telephone number rather than the one provided by the alleged IT employee.

3. A culture of security
It is fundamental to create a work environment in which everyone feels responsible for security, promoting the reporting of suspicious behaviours or requests. No one should feel uncomfortable in saying, "this request seems strange", or asking someone for a second opinion.

4. Protecting devices
Never leave company laptops, smartphones or devices unattended, especially in shared or public areas. Lock your screens with passwords or PIN numbers and ensure that devices lock themselves automatically after a time of inactivity.

5. Two factor Authentication (2FA)
Even if someone is able to obtain an access password, 2 factor authentication provides a further level of security. This tool, which requires a second step to confirm the identity of a user, is essential in protecting company accounts.

6. Controlled physical access
Ensure that only authorized people can enter offices or sensitive areas. Using personal badges, surveillance cameras and electronic doors can be effective ways to prevent physical intrusions.

7. Attention to warning signs
Be attentive to details. Emails with errors in grammar, unusual requests or unknown senders are often warning signs. Before clicking on any links or downloading an attachment, always ask yourself if the request makes sense. In case of any doubt, it is better not to take a risk.

8. Periodic tests and audits
Make regular security audits and penetration tests to identify any vulnerabilities in systems and processes. These tests can reveal weak points that could be exploited by cybercriminals.

Conclusion
Social engineering is an insidious threat, but it is not invincible. Being aware of how criminals work and implementing good practices can significantly lower risks. Investing in employee training, promoting a culture of security and using appropriate tools are crucial steps in protecting sensitive information and critical systems. Security often does not depend merely on technology, but on people's attentiveness and preparation in recognizing scams.

INVISIBLE THREATS: THE INCREASE IN CYBERATTACKS

Introduction

In the digital era, the threat of cyberattacks has become an ever-growing sophisticated danger that is difficult to detect. Organizations from all sectors face attacks targeting sensitive data, operational continuity and business reputation. The increase in these attacks not only results in direct financial damages, but also in lack of trust from clients and partners. This article addresses the main cyber threats, the financial challenges they cause to businesses and strategies to defend oneself effectively.

1. The top cyber threats

Cyberattacks are in continuous evolution and exploit both human and technological vulnerabilities. The following are among the most common threats:

• **Ransomware:** a type of malware that encrypts company data, blocking access until a ransom is paid.

• **Phishing and Spear Phishing**: malicious emails that are aimed at accessing credentials and sensitive data, using social engineering.

• **Zero-Day Attacks:** They take advantage of unknown or unaddressed security flaws in the software before software producers have the opportunity to correct the flaws.

• **Malware and Trojans:** malicious programs that infiltrate systems to steal information or allow unauthorized access.

• **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** attacks that overwhelm business servers making them inaccessible to legitimate users.

• **Credential threats and Violation of Data:** attacks that compromise company credentials to access reserved systems.

2. Financial challenges for Organizations

Cyberattacks are not limited to compromising IT systems, and have significant financial impacts. Among the chief ones are:

• **Recovery costs:** Businesses affected by cyberattacks invest in forensic analyses, data recovery and efforts to strengthen security measures.

• **Penalties and legal issues:** Regulations such as the GDPR apply heavy penalties in cases of personal data breaches.

• **Damages to Reputation:** The loss of trust of clients and partners can drastically reduce the value of a brand.

• **Interruption to operations:** A successful attack can stop business operations for days or even weeks, with significant financial losses.

3. Protection Strategies and Solutions

In order to lower risks, organizations should adopt a cybersecurity strategy that is proactive. The following are some important measures:

• **Training and Awareness:** Educating employees about cyber threats reduces the risk of attacks based on human deception.

• **Implementation of Multi-Factor Authentication (MFA):**Adding a further level of security to access reduces the risk of compromised accounts.

• **Updates and Security Patches:** Always update software and operating systems to protect from exploits.

• **Regular Encrypted Backups:** Backup frequently and store backups in safe places to ensure a quick recovery in case of an attack.

• **Continuous Monitoring and Threat Intelligence:** Use advanced tools to uncover threats in order to identify and quickly respond to suspicious behaviours.

• **Firewalls and Intrusion Prevention Systems (IDS/IPS):** Protect company networks from unauthorized access and external attacks.

• **Zero Trust Architecture:** Adopt a security model that does not consider any access as reliable, requesting constant verification for each data transaction.

Conclusion

Cyberattacks are constantly evolving and can have a significant impact on businesses, both in terms of security and in terms of financial costs. Implementing a proactive approach to cybersecurity, investing in data protection and training employees are essential steps to protect oneself from the invisible threats of the digital world. Only an integrated strategy and constant vigilance can provide an effective protection to business infrastructure and ensure operational resilience.

CYBER SECURITY IN GOVERNMENTS: GLOBAL THREATS AND DEFENSE STRATEGIES

In recent years, digitalization has transformed the way governments operate, introducing new opportunities but also new vulnerabilities. Cyber security has become an essential pillar for national stability with public administrations facing increasingly sophisticated and targeted attacks. The management of sensitive data, the control of critical infrastructures and the provision of essential services make government bodies targets of cyber attacks with geopolitical, economic and social implications.

The cost of cyber attacks in the public sector continues to grow, with studies highlighting a financial impact of billions of dollars every year. A case in point is the case of the Irish health service, paralyzed by a ransomware attack in 2023 that caused damages exceeding one hundred million euro. Incidents of this magnitude are not limited to an economic issue but raise questions of trust and public safety. When citizens' personal information is compromised, the perception of vulnerability spreads quickly, undermining the relationship between the state and its citizens. A government's reputation can be severely damaged by a cybersecurity breach. In 2020, an attack on Norwegian healthcare systems exposed personal data of nearly three million citizens, drastically reducing uptake of public digital services. The fear that personal data could be stolen or manipulated inhibits innovation and hinders the adoption of digital technologies with direct repercussions on the modernization of public administration and any government organization.

Defense strategies require a multi-layered approach in which prevention and incident response play a crucial role. Many systems used by government agencies are technologically obsolete, a factor that amplifies the risk of attack. Modernization of IT infrastructure must become a priority, accompanied by rigorous security policies and continuous training of staff. Human error remains a major cause of cyber attacks, making awareness programs and attack simulations essential to improve the capability of responding to threats.

Cybersecurity is not just a technical problem but a matter of national security. Attacks on critical infrastructure can have devastating effects as demonstrated by the case of the Colonial Pipeline in the United States where a cyberattack interrupted the supply of fuel to entire regions. International cooperation is essential to counter large-scale threats as cybercriminals operate without borders. Sharing information between governments and security agencies allows them to anticipate threats and improve overall resilience.

The landscape of government cybersecurity is constantly evolving with threats that rapidly adapt to new defense measures. Investing in the protection of data and critical

infrastructure is no longer an option but an essential necessity to guarantee the stability and security of institutions. In an increasingly interconnected world, protecting cyberspace become equivalent to protecting democracy itself.

Valerio Mercuri

YOUNG PROTAGONISTS OF GLOBAL ETHICS: CYBER DIPLOMACY, LAW, ECONOMICS AND TECHNOLOGY IN AN INTERCONNECTED WORLD

How to distinguish a real fact from a deepfake? Who guarantees that an algorithm does not manipulate public opinion? These questions guided the debate "Cyber Diplomacy, law, economy and technology in an interconnected world", AI and the Future of Institutions", organized by the Directorate of Telecommunications and Information Services. Through slides, data and practical case studies, students and teachers reflected on a crucial theme: in a hyper-connected world, where artificial intelligence (AI) can create or destroy truth in a few clicks, ethics and knowledge become the only antidote to disinformation.

AI and post-truth: when technology challenges perception

The heart of the debate was the legal/economic impact of cybercrimes and the role of AI in shaping reality. On the one hand, cyber attacks are not only a technological threat but a labyrinth of legal challenges, exponential economic costs and reputational risks. From a legal point of view, jurisdictional conflicts (such as the contrast between the European GDPR and the US Cloud Act) make it difficult to prosecute digital crimes while the lack of binding international treaties leaves room for gray areas exploited by hackers and rogue states.

The economic cost is equally critical: according to recent estimates, cybercrime costs the global economy $8 trillion a year, a figure set to rise with the advent of quantum computing and supply chain attacks. Incidents such as the Colonial Pipeline ransomware (2021), which interrupted the flow of fuel in the US, generated direct losses of $4.4 million, not to mention indirect damage to consumer confidence.

Tools such as deepfakes in voice or synthetic videos threaten to erode trust in institutions: in 2023, fake audio attributed to politicians caused volatility in the markets. On the other hand, AI itself can be an ally: fact-checking algorithms and manipulation detection systems offer hope of control. "The problem is not the technology, but how we use it." "We need clear rules: a deepfake for a film is creativity, to influence elections is a crime"

Digital wisdom: why knowledge is a heritage to be protected

If data is the "new petroleum", the ability to interpret it is where the real wealth lies - protecting it is the great challenge. Interventions have underlined how universities and research centers must train young people not only to program algorithms but to question their social impact.

An example? The European GDPR, which limits the use of sensitive data, is born from an ethical vision: to protect people, not just servers. «Digital wisdom is knowing how to balance innovation and rights», the *Cambridge Analytica* case has stigmatized the still immature legal problem where stolen data have

distorted political campaigns and systemic pro-government hacker attacks have caused dramatic socio-economic impacts.

Reputation and cybersecurity: the human at the center

The reputation of a State or a company is now played online. Attacks like the one on *SolarWinds* (2020), which compromised US government data, demonstrate that malware can be more damaging than a missile strike. But the solution is not only technical: «A firewall does not stop the manipulation of news». We need "holistic strategies":

- Transparent platforms that combat disinformation without censoring;
- Education in critical thinking, the ability to discern and recognize fake news;
- International collaboration and legislation, the new frontiers to focus on.

The role of young people: guardians of a "human" future

In closing, the appeal to digital natives: «We live in the first generation that can use AI to amplify knowledge, not to divide it». There is no shortage of concrete examples: startups led by under 30's develop tools to verify journalistic sources, while others design ethical chatbots that refuse to generate hate speech.

The meeting provided simple but urgent messages: in an era in which AI can make falsehoods more convincing than truth, defending the truth is a collective responsibility, Cyber-Diplomacy is essential to reduce the political/economic impacts with potentially devastating social effects.

And young people, with their technological familiarity and sensitivity to values, are called to lead this silent battle, regulate it and normalize it. Not with apocalyptic rhetoric, but with daily and technological choices: sharing news only after having verified it, demanding transparent algorithms, defending knowledge as a common good. Because, as a proverb reinterpreted in a digital key reminds us: Truth is like water: it always finds its way . But someone is needed to clean its banks.

Valerio Mercuri