Securing electronic devices and countering security breaches

Training Content for Parents

Trainer's Booklet

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Securing electronic devices and countering security breaches

Training Content for Parents

Trainer’s Booklet

Intellectual Property rights

December, 2023
Doha, Qatar

This content is produced by the team of
National Cybersecurity Excellence Management, National Cyber Security Agency.

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:

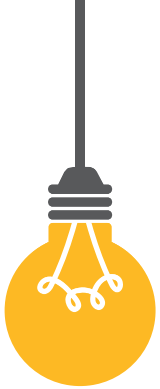
الوكالة الوطنية للامن السيبراني
National Cyber Security Agency

🌐 https://www.ncsa.gov.qa/
✉ cyberexcellence@ncsa.gov.qa
☎ 00974 404 663 78
☎ 00974 404 663 62

General content of the Kit

First: General Introduction to the training kit

Second: Scientific content



First: General Introduction to the Training Kit

Below is an explanation of some details relevant to the objectives of the training kit, along with general guidelines for the trainer on how to handle this kit, while providing him with the scientific content that will be relied upon during the training.

General Idea

The concept of this training kit is to equip the trainer with tools and training resources, making it easier for him to deliver information to the trainees. In general, each training material consists of two parts: One part for the trainee and another for the trainer. The training kit serves as a general guide and support for the trainer, and its scientific content is the same as that of the trainee, but here the training content is presented differently. Additionally, the kit equips the trainer with training tools and methods that support him in the training process.

Objectives of the Training Kit

- Providing the trainer with training tools that help him deliver the training content to the Trainees.
- To present information and training content in an easy and simple manner.
- To offer training content on protection of electronic devices along with multiple training tools and methods.

Contents of the Training Kit

The training kit includes several training tools, as detailed below:

1. **Presentation files.**
2. **Instructional videos.**
3. **Training cards,** comprising general information accompanied by illustrative images, presented by the teacher to the Trainees.
4. **Sketches** containing information on the key subjects covered in the training content.

Content of the Training Kit

WorkShop Timetable

Content	Allocated Time
General introduction	10 minutes
The theoretical aspect	30 minutes
Educational Videos	30 minutes
Short break	20 minutes
Dialogue and discussion with trainees	30 minutes
Total training time	2 hours

Trainer’s Guidance Manual

The following is an explanation of some general guidelines for the trainer, revolving around how to use this training kit:

- The scientific content may encompass concepts beyond the trainees’ expertise, necessitating the instructor to present the information in layman’s terms.
- The instructor projects presentation slides for each topic under discussion. For instance, when explaining the concept of Securing electronic devices, the relevant slide is displayed.
- The instructor presents the”sketches”. section on the screen in front of the trainees during the intermissions between each chapter throughout the training.
- While presenting the scientific material for each chapter, a specific time period is designated to present several links associated with the chapter’s content.
- The trainer presents the videos referenced in a separate file to the Trainees at the conclusion of each chapter or at the time deemed suitable.
- engage in discussions with the Trainees at times you consider suitable.

Second: Scientific Content

Introduction

Securing electronic devices and networks, and consequently, securing information and data from violation and destruction, constitutes the tasks performed by cybersecurity. This applies to both individuals and enterprises. Cybersecurity has expanded into various domains, offering protection against the escalating instances of electronic crimes in recent years, driven by the digital revolution witnessed globally.

Security here is not limited to electronic devices; it is an integral part of the security that users should have online. It encompasses sucuring vital data and information, such as financial matters and personal identifiers, which pose a threat to individuals or enterprises if disclosed and made public. This includes personal data stored on smartphones or computers. In this context, cybersecurity plays a crucial role in countering such threats through electronic defense programs, preventing issues from arising. Cybersecurity preserves the security of society, its individuals, and their data.

One of the electronic attack tools affecting devices and software, facilitating their compromise, is 'malicious viruses.' These aim to deceive and cause damage, resulting in financial and data losses. The impact extends beyond data theft and fraud; these viruses also lead to data destruction by corrupting all files associated with individuals or enterprises, as well as damaging the devices. This consequently causes significant material and moral losses due to the disruption of operations built upon these systems and data.

The primary reason for the escalation of cybercrimes is the connection of a staggering number of devices to the internet, reaching approximately 21.1 billion devices in 2021. Phishing through the dissemination of harmful links via email was a prominent form of these crimes. Additionally, ransomware programs, which restrict users from accessing their files on the device, necessitating the payment of a ransom to the criminal for file retrieval, were prevalent. Numerous other forms of threats, scams, and causing harm to others were also observed.

Chapter One

The Significance of Electronic Device and Network Security.

- First: The Significance of digital stability for networks and connected devices.
- Second: Digital threats in digital devices (phones, computers, tablets)

0 1

First: The Significance of digital stability for networks and connected devices

The digital environment has witnessed rapid development, with the prevailing trend in the new information landscape being the swift growth of digital data and internet resources, and the continual expansion of the global communication network. The digital environment encompasses the entire spectrum of computer and network technologies.

The fundamental structural component of the global digital environment is comprised of networks and communication systems. It is noteworthy that the global volume of information doubles every two years, and according to Cisco, the global IP traffic surpassed approximately 3.3 zettabytes (a zettabyte equals one billion gigabytes) in 2021. It can be acknowledged that digital networking technologies are deeply intertwined with the fabric of educational, productive, and representational processes.

The World Wide Web primarily utilizes this to establish a shared digital environment (infrastructure) for connecting machines, equipment, infrastructure facilities, transportation, logistical chains, organizations, and intended users.[1]

The expansion of the digital environment, coupled with the emergence and spread of new networking and information technologies, has led to both numerical and qualitative growth in various risks and threats faced by individuals and societies. Objectively, this will result in the emergence of different types of information security threats. Information security threats have increasingly become an urgent issue, and according to many experts, one of the highly interdisciplinary tasks of this century is to confront these threats and manage technological risks.

1. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97–106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088.

The widespread use of information and communication technology, the expansion of the networked information environment, the inherent interactivity of the internet, and the emergence of social networks lead to new risks and threats to information security. This indirectly contributes to social instability, as the widespread use of modern networking technologies creates potential prerequisites for such threats. Examples of these threats include information leakage, theft, defamation, duplication, impersonation, and denial-of-service attacks, resulting in economic, environmental, social, and various other forms of damage.

Through their unauthorized access of computer networks, criminals not only copy the stored information but also corrupt it with viruses that can destroy application or system programs that respond after a certain period (or under specific conditions), making it difficult to identify the perpetrators.

According to Positive Technologies, the cyber threat statistics for the year 2018 were as follows: The percentages of targeted attacks, attacks aimed at stealing personal, accounting, and payment card data were 62, 30, 24, and 14%, respectively. Malware was used in 56% of cyber attacks.[1]

Furthermore, the advent of the internet of things has cast its shadows on cybersecurity risks for individuals. According to studies conducted by the Massachusetts Institute of Technology, instances of disruptions and consecutive failures due to software errors and defects will become a routine part of our daily lives, reaching dozens or hundreds of cases each year. Consequently, the potential economic and social risks of the internet of things lie not only in the exploitation by unauthorized entities but also in its very existence and ongoing development.

[1] Ibrahim, Hamadi Osman. Information Security, Computer Science Lectures, Department of English, College of Humanities, Al-Anbar University, Iraq. available on the link: https://www.uoanbar.edu.iq/eStoreImages/Bank/1352.pdf.

Information security

It refers to the means, tools, and procedures necessary to ensure the protection of information from internal and external threats. It is the discipline that studies how to provide confidential and secure protective measures for information and how to counteract attacks on it.

Information security relies on several steps to ensure the protection of devices and networks from unauthorized access. These include:

- Utilizing the username and password.
- Securing the computer from hackers using antivirus software.
- Securing software, data, and backups.
- Utilizing a firewall.[2]

Network Security

It is part of the information security system that focuses on securing the use and integrity of the network, and consequently, the integrity of data. This field encompasses both hardware and software technologies. Network security effectively manages network access, targeting and preventing a diverse range of threats from entering or spreading within your network.

Network security integrates multiple layers of defenses, where each layer executes policies and control elements. As a result, authorized users can access network resources, while malicious actors are prevented from executing exploitation operations and threats.

Network security programs are based on several fundamentals, the most important of which are explained below:

1. Access Control

It refers to enforcing security policies that prevent unauthorized users from accessing and, consequently, gaining entry to your network, devices, and data. Network owners can, for example, block incompatible endpoint devices or grant them only limited access. This process is referred to as ‘network access control’.

2. Antivirus and anti-malware programs

Malicious software, known as Malware (an abbreviation for malicious software), encompasses viruses, worms, Trojans, ransomware, and spyware. While malware can sometimes infect the network, it often remains dormant, or asleep, for days or even weeks. This is where the importance of antivirus and anti-malware programs comes in, as they scan for and remove harmful programs, repairing any damage.

3. Application Security

Application security encompasses the hardware, software, and processes used to close vulnerabilities in applications.

4. Behavioral Analysis

Behavioral analysis tools automatically distinguish suspicious activities for prompt processing.

5. Data protection

Data Loss Prevention (DLP) technologies prevent individuals from uploading, redirecting, or even printing sensitive information in an insecure manner.

6. Email Security

Email Security is essential, considering that email is one of the primary channels through which attackers gain unauthorized access to devices, aiming for ransom, extortion, and phishing scams. Therefore, Email Security applications prevent incoming attacks and regulate outgoing messages to prevent the loss of sensitive data.

7. Firewalls

Firewalls create a barrier between your trusted internal network and untrusted external networks, such as the internet; they use a set of defined rules to allow or block visits.

8. Spy prevention systems

Intrusion Prevention System (IPS) examines network visits and traffic to prevent attacks effectively.

9. Mobile Device Security

Cybercriminals increasingly target mobile devices and applications, so there is a growing need to control the devices that can access your network.

10. Network Segmentation

Network segmentation software classifies network traffic into different categories. This allows network owners to grant the appropriate level of access to the right people and to identify and address suspicious devices.

11. Web Security

A web security solution will prevent web threats and prevent access to malicious websites.[1]

[1] What Is Network Security? cisco. On site: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

Second: Digital threats in digital devices (phones, computers, tablets)

Digital devices are subjected to a range of challenges and risks; the most important of which are outlined below

1. Data leak

Sometimes, mobile device applications can unintentionally lead to data leakage. For example, 'malicious' applications, which often come as free applications, pose a real problem for mobile device users who grant them extensive permissions without always verifying their security. These applications may send personal and, perhaps, work-related data to a remote server, providing an opportunity for cybercriminals to exploit. To avoid this issue, only grant applications the absolutely necessary permissions and ignore any program that requests more than necessary.[1]

2. Network spoofing

Public Wi-Fi networks are often insecure, and to protect against electronic attacks, users should rarely use free Wi-Fi on their mobile devices and should never use it to access sensitive or personal services, such as banking information or credit card details.

Network spoofing occurs when hackers set up fake access points that appear to be public Wi-Fi networks, but are actually traps, often found in places like cafes, libraries, and airports. Cybercriminals typically give these access points generic names such as 'Free Airport Wi-Fi' or 'Café' to entice users to connect to them.

The attacker may require users to create an 'account' to access these free services, completing the process by requesting a password. As many individuals tend to reuse the same password and email for logging into multiple accounts, these hackers can gain access to all private data.[2] Therefore, caution is advised when connecting to any public Wi-Fi network. If prompted to create a login, always choose to enter a different password.

[1] Mobile Cyber Threats, Kaspersky Lab&Interpol Joint Report. On site: https://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf.

[2] Mouselly, Tariq. 7 Security Threats When Using Public Wi-Fi (And How to Protect Yourself), Information Security, 2021, available on the link: https://cutt.us/cb7w0.

3. Phishing Attacks

Mobile devices represent the front lines for phishing attacks, as they are constantly in operation. Therefore, users of mobile devices are more vulnerable to attacks, often being the first recipients of seemingly legitimate email messages and falling for the bait. Thus, it is crucial never to click on unfamiliar email links, especially as verifying them becomes more challenging on the small screens of mobile devices. It is advisable to manually enter URLs whenever possible to ensure safety.

4. Spyware

Often, it is not malware that users should be cautious of, but rather spyware. To protect devices from it, it is essential to download an effective suite of antivirus and anti-malware programs and eliminate them before they have the opportunity to collect your personal data.

5. Compromised encryption

Compromised encryption may occur when application developers employ encryption algorithms that are either weak or utilize strong encryption without proper implementation processes. In the former case, developers may use encryption algorithms known to have existing security vulnerabilities in order to expedite the application development process. Consequently, this could allow attackers to compromise passwords and gain unauthorized access to desired information on the devices. In the second scenario, developers employ highly secure algorithms, but they leave other 'vulnerable entry points' that diminish their effectiveness. For instance, Attackers may not be able to crack passwords, but if developers programming errors that allow attackers to modify high-level application functions, such as sending or receiving text messages, then they do not require passwords to cause issues for users.[1]

Overall, the nature of security threats to mobile devices has undergone significant changes, with three key areas being particularly impacted:

- **Desktop computers,** Computers are highly vulnerable to hacking threats, and they are also considered a gateway to hacking smartphones and tablets, as hacking infections may be transmitted from computers to other devices connected to them.

[1] Broken cryptography, resources. On site: https://cutt.us/an1BC.

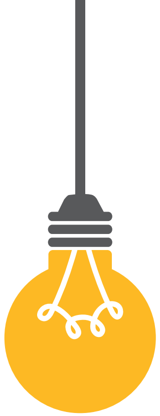
- **Smartphones and tablets:** Smartphones and tablets face more hacking threats than computers, due to the fact that protection programs designed for smartphones and tablets are less advanced and efficient than those designed for computers.
- **Expanding range of smart devices:** In light of the rapid technological development, the spread of smart devices in homes and in the business environment has increased, especially devices associated with smart homes. This multiplicity of smart devices increases the chances of being hacked, especially since these devices are often connected to each other, so hacking one of them means transmitting the hack to the rest. Devices.[2]

[2] Top Trends and Threats in Mobile Security: Gartner, cxotoday. On site: https://cutt.us/oMMsw.

Chapter Two:

Types of digital threats in devices

- First: Ransomware attack.
- Second: Device data theft.
- Third: Unauthorized access.
- Fourth: Malware.



02

First: Ransomware attack

Ransomware

These are malicious programs designed to prevent users or enterprises from accessing files on their computer devices. By encrypting these files and demanding a ransom in exchange for a decryption key, cyber attackers place individuals and enterprises in a position where paying the ransom becomes the easiest and most cost-effective way to regain access to their files.[1]

Ransomware is considered the most prominent and evident type of malicious software, as it impacts the ability of vital institutions, such as hospitals, to provide essential services, resulting in significant damage.

What are the reasons for the widespread spread of ransomware attacks?

The rapid spread of ransomware attacks accelerated with the emergence of the WannaCry virus in 2017, which garnered global attention due to the widespread damage it caused. Additionally, the COVID-19 pandemic has also contributed to the recent surge in ransomware incidents, as individuals and enterprises rapidly shifted towards remote work, resulting in vulnerabilities in their cybersecurity defenses. Cybercriminals exploited these vulnerabilities to deploy ransomware.

For example, in the third quarter of 2020, ransomware attacks increased by 50% compared to the first half of that year. This period coincided with the global spread of the pandemic, leading to increased reliance on the internet for both professional and personal tasks to avoid social interaction. Ransomware were also identified in 25% of all cyber violations in 2022, according to a report by the telecommunications giant Verizon. Additionally, a Sophos report revealed that ransomware impacted 66% of enterprises in 2021, marking a 78% increase from the previous year.[2]

[1] Ransomware - Definition, Prevention, and Removal, Kaspersky. available on the link: https://cutt.us/G5L3h.

[2] Al-Shamikh, Iman. Losses in the millions... How did ransomware viruses ignite fires in the world of technology? May 2023, Al Jazeera. Available on the link: https://cutt.us/2szL7.

There are dozens of types of ransomware, each with its own characteristics. Some of these include:

1. Ryuk

This ransomware operates through phishing emails or by using compromised user credentials to log into its systems or those of the affected enterprise. Upon infecting the system, Ryuk encrypts specific types of files and then demands a ransom. It is one of the most destructive ransomware, requesting an average ransom exceeding one million dollars.

2. Maze

This ransomware is renowned for being the first to combine file encryption with data theft. It operates by collecting sensitive data from the victims' computer systems before encrypting it. If ransom demands are not met, it publicly exposes or sells this data to the highest bidder.

3. REvil

It is another form of ransomware that targets large enterprises. Cybercriminals employ the technique of double extortion to steal data from companies while also encrypting files. This means that, in addition to demanding a ransom for decrypting the data, they threaten to release the stolen data if a second payment is not made.

4. LockBit

This data encryption malware has been in operation since September 2019. This specific type of ransomware was developed to swiftly encrypt data for large enterprises, as a means to evade detection by security devices and IT teams.

5. Dear Cry

In March 2021, Microsoft released patches for four security vulnerabilities within Microsoft servers. This ransomware program was designed to exploit four recently disclosed security vulnerabilities in Microsoft Exchange. It works by encrypting specific types of files and then sending a ransom message, instructing users to send an email to the ransomware operators to learn how to decrypt their files.

6. Lapsus

This is a ransomware group in South America linked to cyberattacks on some prominent targets. It is notorious for extortion, threatening to release sensitive information. It has previously hacked Samsung, concealing malicious software files as trustworthy files.[1]

[1] What is Ransomware? checkpoint. On Site: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

How ransomware operates

For ransomware programs to successfully achieve their malicious goals, they require access to the targeted system, encrypt its files, and then demand a ransom from the victim. **There are three fundamental stages in this process:**

1. Infection vectors and dissemination

Like any malware, there are a number of ways to gain access to a targeted victim's system, whether an individual or an enterprise. However, ransomware operators tend to use a small number of specific infection vectors, or channels of infection. One of their preferred channels is phishing emails.

The malicious email may contain a link to a website hosting a harmful download or an attachment with an embedded download function. If the email recipient falls victim to the phishing attempt, the ransomware program is downloaded and executed on their computer.

2. Data encryption

Once cybercriminals gain access to the computer system, whether for an individual or an enterprise, they initiate the encryption of files using a key controlled by the attacker. The original copies are replaced with encrypted versions, and these files are often carefully selected to ensure system stability. The goal here is financial gain rather than outright system destruction.

3. Ransom demand

After completing the file encryption process, the ransomware program is ready to issue a ransom demand. Various variants of ransomware achieve this in several ways, typically requesting a specified amount in cryptocurrency in exchange for access to the victim's files. Upon payment of the ransom, the ransomware operator facilitates the victim's access to their files for reuse.[1]

[1] How Ransomware Works, unitrends. On Site: https://www.unitrends.com/solutions/ransomware-education.

How to protect against ransomware

Effective preparation can considerably mitigate the cost and impact of a ransomware attack. Adhering to the best practices outlined below can assist both individuals and enterprises in diminishing their vulnerability to ransomware and mitigating its repercussions. The subsequent steps represent key measures to curtail the risk of a ransomware attack

- **Instruction, training, and awareness on digital security and concepts of cybersecurity**

Ransomware frequently disseminates through phishing emails. Consequently, it is recommended to undergo training on recognizing potential ransomware attacks and mitigating their occurrence.

- **Regular data backup**

Ransomware is a type of malicious software that encrypts a victim's files, rendering them inaccessible until a ransom is paid. As a result, automatic data backups can assist users in recovering from an attack with minimal data loss and without the need to pay a ransom.

- **Patching**

The timely application of software patches is a fundamental aspect of cybersecurity defense against ransomware attacks. Cybercriminals frequently target systems with unpatched vulnerabilities. Therefore, enterprises and individuals must diligently apply the latest patches to all systems to minimize exploitable vulnerabilities.

- **User Authentication**

Gaining access to certain services through the utilization of stolen user credentials is a prevalent tactic employed by ransomware attackers. Consequently, the implementation of strong user authentication mechanisms serves as a crucial countermeasure to protect against the exploitation of compromised or stolen passwords.

- **Reducing the Attack Surface**

Prevention is the best strategy to mitigate the impact of ransomware, and this can be achieved by reducing the attack surface through addressing:

- Phishing messages.
- Unpatched vulnerabilities.
- Remote access solutions.
- Mobile malware.[1]

[1] What do I do to protect against Ransomware? security.berkeley.edu. On Site: https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware.

How to mitigate active ransomware infections

A significant percentage of successful ransomware attacks remain undetected until the encryption of data has been completed and a ransom demand is displayed on the screen of the compromised computer. At this stage, the encrypted files are beyond recovery; however, **prompt action is imperative to mitigate the repercussions of the attack:**

- **Isolating the device:** Some forms of ransomware have the capability to spread to connected drives and other devices. To prevent this, it is crucial to isolate the infected device from other connected devices.
- **Maintain the computer in an operational state:** File encryption can render a computer unstable, so shutting down the computer is not a guaranteed solution, as it may result in memory loss.
- **Creating a backup:** Create a copy of the encrypted files on removable storage.
- **Ensure the availability of decryption tools:** Check the No More Ransom Project to determine the availability of a free decryption tool. If available, execute it on a duplicate of the encrypted data to assess its capability to recover the files.
- **Seek assistance:** Computers often store backup copies of their files, and a specialist can assist in recovering these copies if they haven't been deleted by malware.
- **Reformat and Restore:** Recover the device using a previously saved clean backup or reinstall the operating system to ensure that the malware is completely removed from the device.[1]

[1] Mitigating malware and ransomware attacks, how to defend organisations against malware or ransomware attacks. On Site: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

Second: Device data theft

Definition of Data Theft

The unauthorised acquisition of data, also known as information theft, involves the unlawful transfer or storage of personal, sensitive, or financial information. This can encompass passwords, source code, algorithms, processes, or proprietary technologies. It constitutes a grave breach of security and privacy.

To elaborate, data theft constitutes the illicit acquisition of digital information stored on computers, servers, or electronic devices with the intent to procure confidential data or infringe upon privacy. Upon gaining unauthorized access to such information, the perpetrator can manipulate it by deleting, altering, or restricting access without the owner's consent.

Data theft commonly occurs when malicious actors intend to sell the information or utilize it for identity fraud. It does not literally imply the physical removal of information from the victim; instead, the attacker merely replicates or duplicates the information for their own purposes.

Data theft is also known as a 'data breach' or a 'data leak', but there are nuanced distinctions between these concepts. These are:

- Data leaks occur when sensitive information is inadvertently revealed, either online or via misplaced or lost hard drives or devices. This implies that cybercriminals can acquire unauthorized access to sensitive data without exerting any effort.
- Data hacking refer to deliberate cyberattacks.[1]

[1] Al-Akaila, Abdullah Majid Abdul Muttalib. Data and Electronic Information Theft: A Comparative Study, College of Sciences and Humanities - Department of Law, Prince Sattam bin Abdulaziz University. Available on the link: https://jfslt.journals.ekb.eg/article_10943_869bcc9f604774fe726ffe0bc9e5878b.pdf.

How does data theft occur?

Data theft can be perpetrated using a diverse range of tools. **The following are some of the most commonly employed:**

1. Social engineering

The most common form of social engineering is phishing, occurring when the attacker disguises themselves as a trusted entity to deceive the victim into opening an email, text message, or instant message.

2. Weak Passwords

Using a weak password or employing the same password for multiple accounts can allow attackers to access data. Additionally, poor password habits, such as writing passwords on a piece of paper or sharing them with others, can also result in data theft.

3. System Vulnerabilities

Inadequately designed or implemented software applications or network systems can engender security vulnerabilities that can be leveraged by attackers to steal data. Additionally, outdated antivirus software can also create security vulnerabilities.

4. Internal Threats

Employees within an enterprise may possess access to customers' personal information, which could be exploited.

5. Human error

Occasionally, data theft can arise from human error, such as sending sensitive information to the wrong person, inadvertently emailing to an incorrect address, attaching the wrong document, or delivering a physical file to an unauthorized individual.

6. Installing software from untrusted sources

Acquiring software or data from compromised websites, such as those plagued by viruses, mobile viruses, or malware.

7. Loss of electronic devices.

Not all data theft incidents are attributable to cybercrime. Some instances involve the physical theft or loss of electronic or paper files, or the theft or loss of electronic devices. The growing prevalence of remote work has also increased the likelihood of device loss or theft. If you work in a public place, such as a café, someone may be able to observe your screen and keyboard to steal information, such as your login credentials.

8. Publicly Available Information

Many pieces of information can be discovered through online search operations and by examining user posts on social media platforms.[1]

[1] What is data theft and how to prevent it, Kaspersky. On Site: https://www.kaspersky.com/resource-center/threats/data-theft.

What types of data are typically stolen?

1. Customer records.
2. Financial data, such as credit card or debit card information.
3. Source codes and algorithms.
4. Descriptions of ownership processes and operational methodologies.
5. Network credentials, such as usernames and passwords.
6. Human resources records and employee data.
7. Private documents stored on computers.[1]

Data theft consequences

Individuals engaged in data theft may be subject to the following consequences:

1. Potential legal claims from clients whose information has been disclosed.
2. Ransom demands from attackers.
3. Recovery costs, such as restoring or patching compromised systems.
4. Defamation and loss of customers.
5. Fines or penalties from regulatory bodies depending on the industry.
6. Interruptions during data recovery.
7. For individuals whose personal information has been breached, the primary consequence is the potential for identity theft, which can result in financial losses and emotional distress.

[1] The 5 most common types of data stolen, Lewis Morgan, March 2014. On Site: https://www.itgovernance.co.uk/blog/the-5-most-common-types-of-data-stolen.

How to keep data secure

Data security can be maintained by adhering to the following:

1. Utilize strong passwords

Intruders can effortlessly compromise passwords if you do not employ a strong password. Consequently, your strong password should be at least 12 characters or more in length, and comprise a combination of uppercase and lowercase letters, along with symbols and numbers.

2. Avoid utilizing the same password for multiple accounts.

Should you employ the same password for multiple accounts, a successful intrusion into one website by a hacker could grant them access to several other sites. Therefore, it is prudent to regularly update your passwords.

3. Avoid writing down your passwords

Writing passwords in any form renders them vulnerable to interception by unauthorized individuals, regardless of whether the medium is a physical document, an Excel spreadsheet, or the Notes application on your mobile device.

4. Multi-Factor Authentication

It is a tool that affords internet users an enhanced degree of account security beyond the traditional combination of email address and password. Two-factor authentication necessitates the employment of two distinct and independent methods to verify identity for accessing a particular service or resource. The first factor is typically the password, while the second typically involves a text message containing a code sent to your smartphone, or your fingerprint, facial recognition, or iris recognition.

5. Limiting the sharing of personal data on social media platforms.

Familiarize yourself with the security settings on each social media platform and ascertain that they are configured to a level that aligns with your preferences to prevent the disclosure of personal information, such as your address or date of birth, on your profile.

6. Close inactive accounts

A considerable number of individuals have registered for online services that they no longer utilize. These services likely hold a combination of personal data and identity details, all of which constitute valuable information for cybercriminals. The situation is exacerbated when the same password is employed across multiple accounts. Therefore, it is strongly advised to remove personal data from unused services and close old accounts rather than leaving them inactive.

7. Deleting Personal Information

Delete messages containing personal details and regularly review your email, as this may bring to light a data breach that may have otherwise gone unnoticed.

8. Update your systems and software regularly

This is accomplished by regularly installing security updates for web browsers, operating systems, and software as soon as they are released.

9. Be careful of free Wi-Fi services

The utilization of free public Wi-Fi has become an ingrained habit for many individuals, however, secure and reliable connections are not always what they appear to be. Public Wi-Fi hotspots can be readily exploited by hackers and cybercriminals who can utilize them to steal data.

10. Antivirus programs

Employing high-quality antivirus software is a cornerstone of maintaining online security. This software assists in identifying vulnerabilities and cyber threats on your device, thwarting them before they can cause harm.[1]

1. 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe. On Site: https://www.digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-online-safe.

Third: Unauthorized access

Unauthorized Access Definition (Illegal Access)

Unauthorized access involves gaining entry to computer resources without authorization. These resources may include a system, network, program, or data. Unauthorized access is typically perpetrated by hackers, but can also occur unintentionally. Individuals with legitimate access to the system may inadvertently encounter insecure files that were not intended for their perusal.

As for how unauthorized individuals gain access to systems and files, the reasons include:

- The user inadvertently guessing the password for sensitive files or data.
- Perpetrating sophisticated attacks that require meticulously planning over several weeks, and may even involve espionage operations targeting enterprises and their users.
- Cybercriminals can go even further in their deception to gain enough trust to appear as authorized individuals.

The risks of unauthorized access

1. Disruption of electronic systems.
2. Causing harm to the target; unauthorized data is typically sensitive and can cause distress or damage to the victim.
3. Data theft, the predominant method employed by individuals seeking to obtain unauthorized access to data for the purpose of executing ransom schemes.
4. Causes material damage to network-connected devices.
5. Defaming enterprises and individuals.
6. Financial and reputational penalties; many enterprises are required to comply with a set of cybersecurity procedures and regulations. When unauthorized cybercriminals gain access to the systems and files of these enterprises, the likelihood of customer harm increases. This can damage the enterprise's reputation and lead to a fine.
7. The escalating costs, as institutions strive to patch vulnerabilities and damages resulting from unauthorized access to their systems and files, compel them to make additional payments and incur expenses amounting to tens of millions of dollars.[1]

Instances of unauthorised access

1. **The theft of an individual's access card is** technically considered unauthorized access. Subsequently, the perpetrator may steal office laptops or compromise any mainframe computer.
2. **Exploiting security vulnerabilities,** as hackers tend to be skilled and patient, meticulously exploring the digital networks of individuals and enterprises to identify vulnerabilities and exploit them.
3. **Social engineering**, meaning the deception of an individual to engage in something harmful to oneself or their devices. All that is required is a well-crafted and carefully designed email or a repeated website to deceive someone into submitting their username and password.

[1] What is unauthorized access? nordvpn. On Site: https://nordvpn.com/blog/unauthorized-access/.

Tips for detecting and preventing unauthorized access.

1. Implementing a strong and complex password policy.

You should never use the word 'password' as your password. It is not only a common password but also the most widely used one. As a result, an intruder needs less than a second to identify some of the most common passwords. It is advisable not to use birthdates or anything that identifies your identity or family.

2. Regular prompts and verifications concerning cybersecurity procedures.

The best way to train on new practices is through routine, as regular reminders to all users about security practices consistently enhance cybersecurity significantly.

3. Smart data storage.

One of the most effective ways to prevent unauthorized access is to reduce the number of devices that can access sensitive data, such as restricting the capability of mobile devices like phones or tablets from accessing specific parts of the network.

4. Monitor digital activity on the Internet.

Many data breaches and damages resulting from someone gaining unauthorized access often come from internal users with the intention of complete espionage, aiming to cause the maximum possible harm. Therefore, monitoring user activity makes it easy to detect clear signs of someone looking to create chaos.

5. Secure all endpoints

An endpoint is any location through which a user can access the computer network or system. It is advisable to install antivirus software on each endpoint to remove and detect malicious programs.[1]

[1] Detecting and Responding to Unauthorized Access. Top 8 Practices to Implement, June 28, 2023. On Site: https://www.ekransystem.com/en/blog/detecting-and-responding-to-unauthorized-access.

Fourth: Malware

Definition of malware

It is a comprehensive term that describes any malicious software or code that damages systems. Deliberately seeking to invade computer devices, systems, networks, tablets, and mobile devices, it aims to damage or disable them, often by partially controlling device operations.

The motivations behind malware vary, as it may aim to gain money from you, sabotage your ability to complete work, or simply for bragging rights. While malware cannot physically damage the hardware of systems or network equipment, it can steal or encrypt your data, delete it, alter the fundamental functions of the computer, or seize control over them. It can also spy on your computer activity without your knowledge or consent.[1]

How can I determine if I am infected with malware?

Malware can reveal itself through various abnormal behaviors, and here are some signs indicating the presence of malware on your system:

1. Your computer is performing poorly., as the operating system on your computer experiences a slowdown, whether you are browsing the internet or using your local applications, the utilization of your system resources appears unusually high. You may also notice that your computer's fan is running at maximum speed, indicating that something is consuming system resources in the background. This usually happens when your computer is compromised by a botnet.

[1] . What is meant by malware? support.google.com. Available on the link: https://support.google.com/google-ads/answer/2375413?hl=ar.

2. Your screen is filled with annoying advertisements, and unexpected pop-up ads are a typical sign of malware infection. They are particularly associated with a type of malware known as adware, and usually, these pop-up windows come loaded with other hidden malware threats.

3. Your system crashes, manifesting as freezing or the infamous Blue Screen of Death (BSOD), the latter occurring on Windows systems after encountering a severe error.

4. Mysterious loss of disk space, caused by the presence of bloated malware, hidden in your hard drive and also known as clusterware.

5. An unusual increase in internet activity for your system, for example, when a Trojan gains access to a targeted computer, the next thing it does is access the attacker's Command and Control (C&C) server to download secondary infections, often ransomware, explaining the significant spike in internet activity.

6. Browser settings automatically change. If you notice a modification in your homepage or have new toolbars, extensions, or add-ons installed, you may have some form of malware infection.

7. The antivirus program stops working, and you cannot restart it, leaving you unprotected against deceptive malware that disabled it.

8. Losing access to your files or the entire computer, indicative of being affected by ransomware.(1)

It is essential to note the possibility of powerful malware hiding in your computer without detection. Obtaining malware typically occurs through two common methods: The internet and email; therefore, any time you are connected online, you are vulnerable to risk. In general, malware attacks will not succeed without the targeted user engaging in behaviors that facilitate the breach, such as opening an unknown email attachment or clicking and installing something from an untrustworthy source.

Types of malware

Malware comes in several types, here is an explanation of the most important ones:

1. Adware

They are unwanted programs designed to display advertisements on your screen, often within a web browser. They use deceptive methods, either disguising themselves as legitimate software or exploiting another program to deceive you into installing it on your computer, tablet, or mobile device.

2. Spyware

They are malicious programs that secretly monitor computer user activities without permission and report them to the program's creator.

3. Virus

It is a malicious program that attaches itself to another program, and when unintentionally used, it replicates by modifying other computer programs and infecting them with parts of its own programming instructions.

4. Worms

They are a type of malware similar to viruses that replicate themselves and spread autonomously across systems.

5. Trojans

One of the most dangerous types of malware, often presenting itself as something useful to deceive you. Once it infiltrates your system, the attackers behind the Trojan gain unauthorized access to the infected computer, aiming to steal financial information or install other forms of malware, often ransomware.

6. Ransomware

It is a form of malware that prevents you from accessing your device or encrypts your files, then forces you to pay a ransom to regain access.

7. Exploit

They are a type of malware that exploits errors and vulnerabilities in the system to grant the attacker unauthorized access to your system.[1]

[1] The 12 Most Common Types of Malware, Kurt Baker - February 28, 2023. On Site: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

How to remove malware

Follow these three easy steps to remove malware from your device:

1. Install and download a good anti-malware.
2. Run a scan using your new program.
3. Change all your passwords.

How to protect against malware.

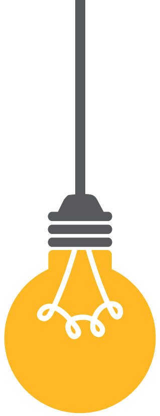
1. Be cautious and attentive if the website is not a top-level domain, such as com, mil, net, org, edu, or biz, for example, among others.
2. Use strong passwords with multi-factor authentication.
3. Avoid clicking on pop-up ads while browsing the Internet.
4. Avoid opening email attachments from unknown senders.
5. Do not click on unfamiliar links that have not been verified in emails, texts, and social media messages.
6. Do not download programs from untrustworthy websites.
7. Adhere to official applications from Google Play and the App Store on Android, OSX, and iOS systems.
8. Ensure that your operating system, browsers, and add-ons are patched and up to date.
9. Remove any programs that you no longer use.
10. Regularly create a backup of your data.
11. install anti-malware software to scan for threats and prevent them from accessing your device.[1]

[1] . How to Protect Your Device from Malware, salamatechwiki. Available on the link: https://cutt.us/ssynj.

Chapter Three

How to Secure Devices from Digital Threats

- First: Passwords
- Second: Data backup



03

First: Passwords

What is password protection?

Password protection helps secure your data from malicious actors by detecting and blocking known weak passwords and terms associated with you. It is an access control technique that assists in securing sensitive data from infiltrators, ensuring that access is only possible through the use of correct credentials.[1]

The Significance of Password Protection

Password protection is one of the most common data security tools available to users. It serves as the first line of defense against unauthorized access to accounts, devices, and files online. Strong passwords help secure data from malicious entities and malware. The stronger the password, the greater the protection of information.

The Consequences of Weak Passwords

For individuals, the loss of personal information can have financial and long-term reputational consequences. When cybercriminals gain unauthorized access to enterprise data, it can result in significant revenue loss, intellectual property compromise, operational disruptions, regulatory fines, and defamation.

[1] What is password protection? Microsoft. On Site: https://www.microsoft.com/en-us/security/business/security-101/what-is-password-protection.

General Guidelines for Creating Strong Passwords

1. Use a minimum of 12 characters.
2. Use a combination of letters, numbers, and symbols.
3. Use at least one uppercase letter.
4. Use a different password for each of your accounts, and change the password from time to time.
5. Use uncommon and unconventional words, such as song lyrics, quotes, or common phrases, to make the password easier to remember, like using the first two letters of each word in the phrase.

Some examples of weak passwords

1. 1234567.
2. 1111111.
3. Password 123.
4. QWERTY.

Second: Data Backup

Having a plan for data backup is one of the most crucial processes to secure data in the event of a cyber attack, whether it's a malware attack or a ransomware attack. With a backup in place, you can run a secure version and restore your data to its previous state. Cloud storage solutions can also be utilized, such as: Google Drive or Dropbox, or by making copies on an external hard drive.

Effective Strategies for Safely Backing Up Your Data

1. 1-2-3 Rule

It refers to creating 3 different copies of your data, placing them on two different types of storage devices, and keeping one copy off-site. **There are several ways to achieve this, as outlined below:**

- Utilize an external hard drive. This can be done by using the built-in backup software on your computer to create a backup of your files on an external storage device. Simply connect the external drive to your computer, and the software will take care of the rest.
- Use an external backup program, and these programs are sometimes faster and more efficient because they leverage cloud-based solutions.
- Copying files manually takes longer for data transfer, but it is a good option if you prefer not to use backup software.

2. **Use a USB flash drive;** portable USB drives are excellent portable storage solutions for storing essential files from your computer, as USB drives are usually much smaller than external hard drives.

3. **Use optical disks,** such as CDs or DVDs, to create a backup of your data; this is an effective method as it provides a tangible backup of your data that you can keep in a secure location.

4. **Use cloud storage;** it is a good method for creating backups as a form of online storage. This service can store files, images, or any other type of data, providing you with a certain amount of space on its servers for a monthly fee. You can access the cloud backup from any computer or mobile device connected to the internet. Cloud storage providers, such as: Google Drive, iCloud, Dropbox, and Backblaze.

5. **Use an online backup service;** you can create a backup of your data using an online backup service by encrypting your files, scheduling regular backups, and storing backup files in a secure location.

6. **Network-Attached Storage (NAS) device**: It is a dedicated server that provides file-level storage and sharing for your home or small business network. It is operational and connected at all times, allowing you to access your data anytime and from anywhere.[1]

In general, backups protect you from data loss in the event of a computer failure or a malfunctioning hard drive. They also provide protection against malware and ransomware if your computer is affected. However, it's crucial to keep your backup plan up to date.

[1] Kyle Chinj How to Back Up Your Data: 6 Effective Strategies to Prevent Data Loss, 2023. On Site: https://www.upguard.com/blog/how-to-back-up-your-data.

Training cards

Pay attention!

Network-Attached Storage (NAS) device

It is a dedicated server that provides file-level storage and sharing for your home or small business network. It is operational and connected at all times, allowing you to access your data anytime and from anywhere.

Pay attention!

Rule 1-2-3

It refers to creating 3 different copies of data, placing them on two different types of storage devices, and keeping one copy off-site. There are several ways to achieve this

- Utilize an external hard drive.
- Use backup software provided by an external entity, such as cloud-based solutions.
- Manually copy files.

Pay attention!

Definition of malware

It is a comprehensive term that describes any malicious software or code that damages systems. Deliberately seeking to invade computer devices, systems, networks, tablets, and mobile devices, it aims to damage or disable them, often by partially controlling device operations.

Pay attention!

Unauthorized Access (Illegal Access)

Unauthorized access involves gaining entry to computer resources without authorization. These resources may include a system, network, program, or data. Unauthorized access is typically perpetrated by hackers, but can also occur unintentionally. Individuals with legitimate access to the system may inadvertently encounter insecure files that were not intended for their perusal.

How to keep data secure

Pay attention

1. Use strong passwords, and change them from time to time.
2. Avoid utilizing the same password for multiple accounts.
3. Avoid writing down your passwords anywhere.
4. Multi-Factor Authentication
5. Exercise caution when sharing personal information
6. Limiting the sharing on social media platforms.
7. Close inactive online accounts.
8. Update your systems and software regularly
9. Be careful of free Wi-Fi services.
10. Utilize Antivirus programs.

Pay Attention!

Data theft

It involves the unlawful transfer or storage of personal, sensitive, or financial information. This can encompass passwords, source code, algorithms, processes, or proprietary technologies. It constitutes a grave breach of security and privacy.

Pay Attention!

Ransomware

These are malicious programs designed to prevent users or enterprises from accessing files on their computer devices, demanding a ransom in exchange for restoring access to their files.

Information security

It refers to the means, tools, and procedures necessary to ensure the protection of information from internal and external threats. It is the discipline that studies how to provide confidential and secure protective measures for information and how to counteract attacks on it.

Pay Attention!

Network Security

Pay Attention!

It is part of the information security system that focuses on securing the use and integrity of the network, and thus the safety of data transfer and exchange processes. This field encompasses both hardware and software technologies. Network security targets and prevents a diverse range of threats from entering or spreading within your network.

Sketches

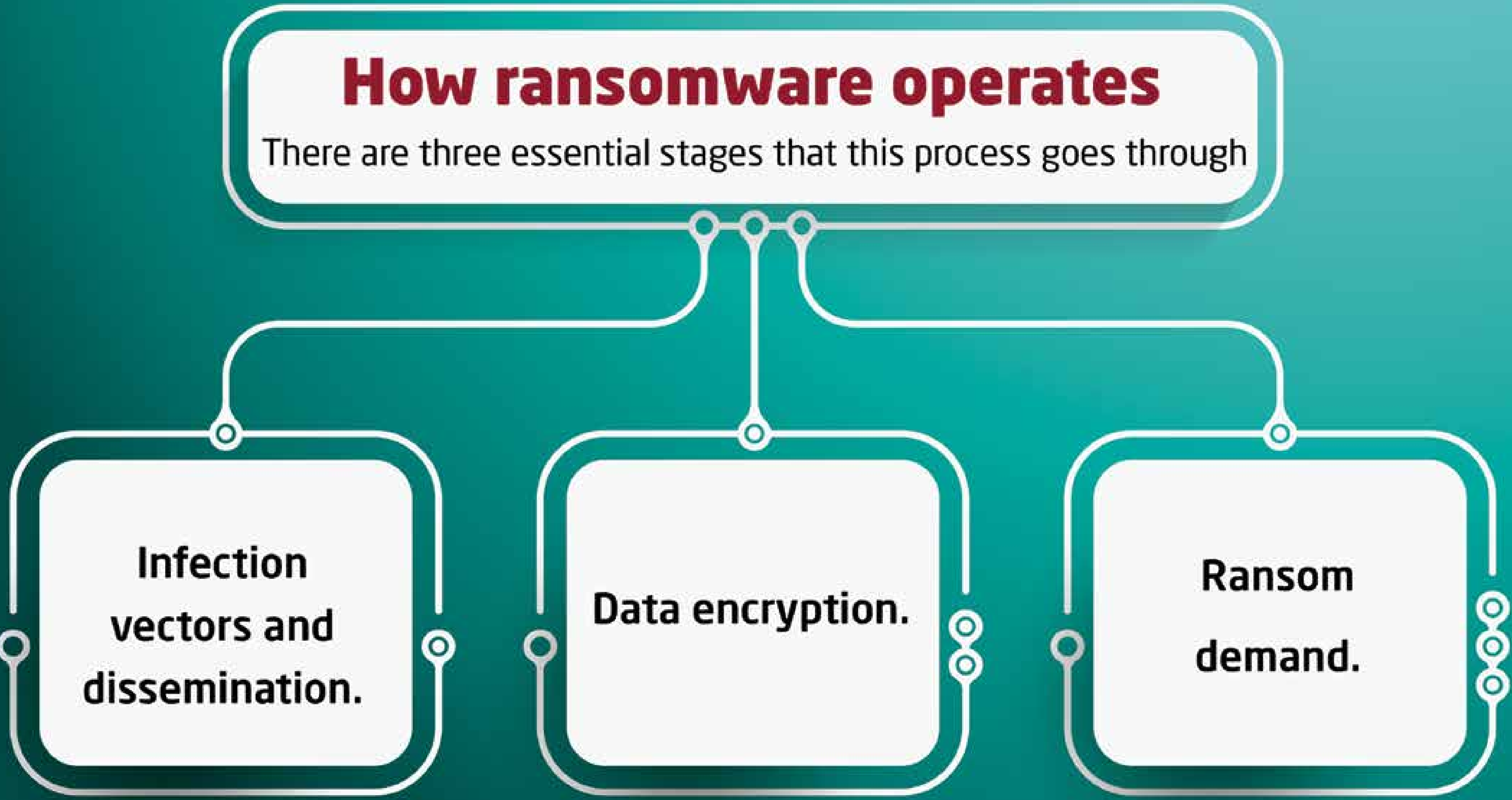
The most prominent digital threats in digital devices (computers, smart phones, Tablets)

01 Data leakage.

02 Network spoofing.

03 Phishing Attacks.

04 Spyware.



How ransomware operates

There are three essential stages that this process goes through

Infection vectors and dissemination.

Data encryption.

Ransom demand.

How to protect against ransomware?

1 Awareness, training, and education on digital security and concepts of cybersecurity.

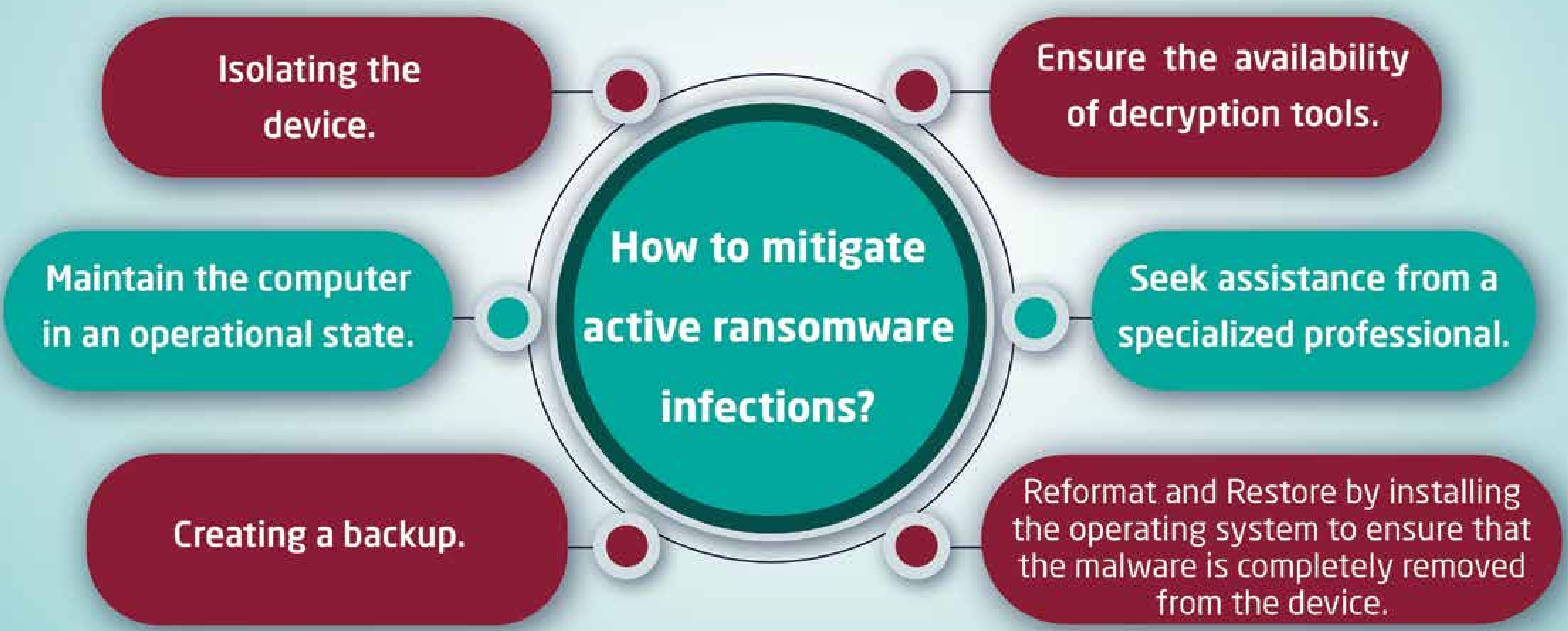
2 Regular data backup.

3 Patching vulnerabilities in systems that have not yet been patched.

4 User authentication mechanisms serves as a crucial countermeasure to protect against the exploitation of compromised or stolen passwords.

5 Reducing the attack surface through addressing

- Phishing messages.
- Unpatched vulnerabilities.
- Remote access solutions.
- Mobile malware.



How to mitigate active ransomware infections?

Isolating the device.

Maintain the computer in an operational state.

Creating a backup.

Ensure the availability of decryption tools.

Seek assistance from a specialized professional.

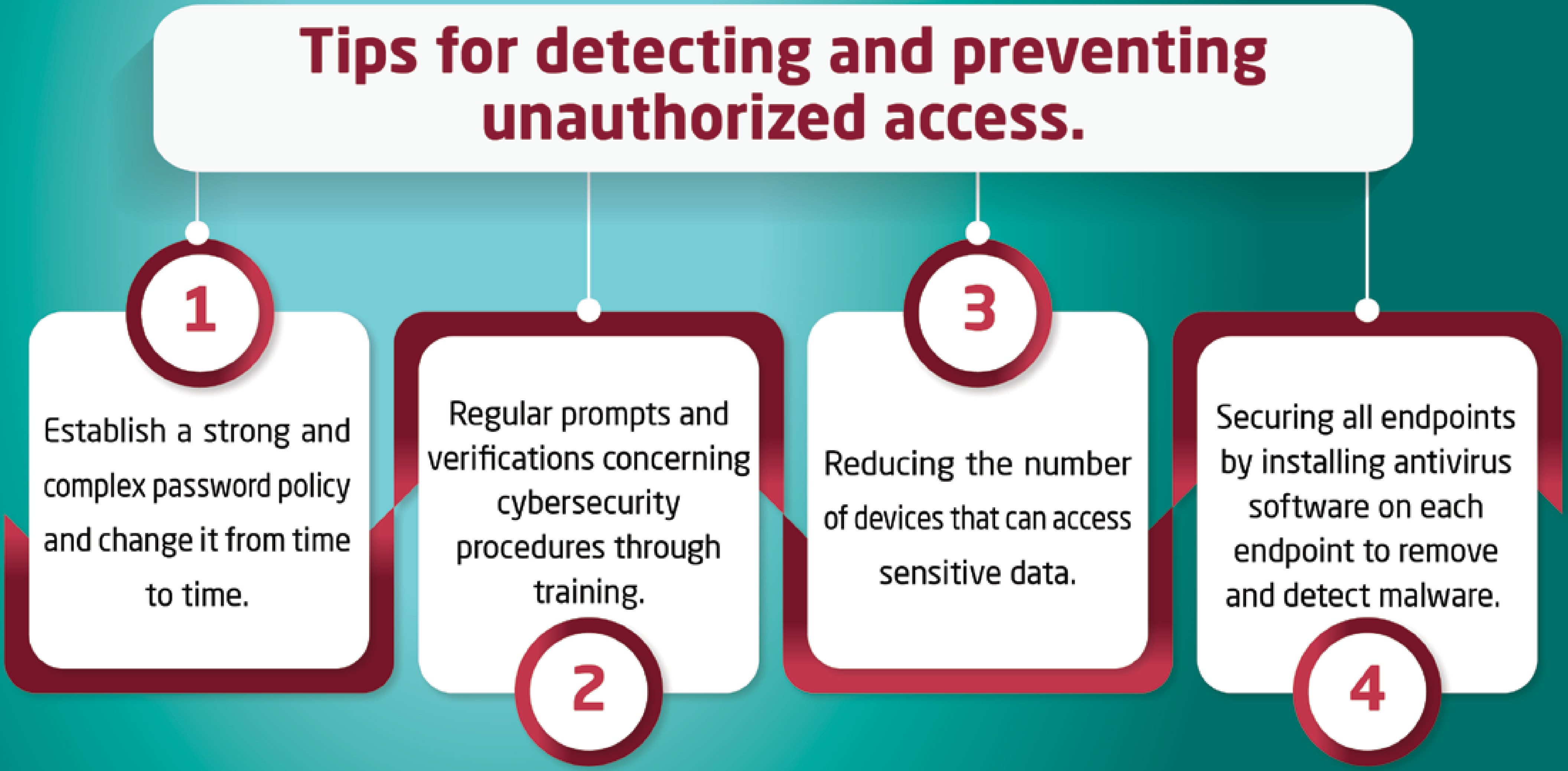
Reformat and Restore by installing the operating system to ensure that the malware is completely removed from the device.

How does data theft occur?

Data theft can be perpetrated using a diverse range of tools.

1. Social engineering.
2. Weak Passwords.
3. System vulnerabilities (security loopholes).
4. Internal threats by certain employees within an enterprise may possess access to customers' personal information, which could be exploited.
5. Human error
6. Installing software from untrusted sources.
7. Theft or loss of electronic devices.
8. Publicly Available Information.

Tips for detecting and preventing unauthorized access.



1. Establish a strong and complex password policy and change it from time to time.

2. Regular prompts and verifications concerning cybersecurity procedures through training.

3. Reducing the number of devices that can access sensitive data.

4. Securing all endpoints by installing antivirus software on each endpoint to remove and detect malware.

How can I determine if my device is infected with malware?

- Your computer is performing poorly.
- The appearance of disruptive advertisements on the screen. Your system crashes, manifesting as freezing or the infamous
- Blue Screen of Death (BSOD), the latter occurring on Windows systems.
- Mysterious loss of disk space.
- An unusual increase in internet activity for your system.
- Browser settings automatically change.
- The antivirus program stops working.
- Losing access to your files or the entire computer.

How to remove malware

1

Install and download good cybersecurity software to combat viruses and malware.

2

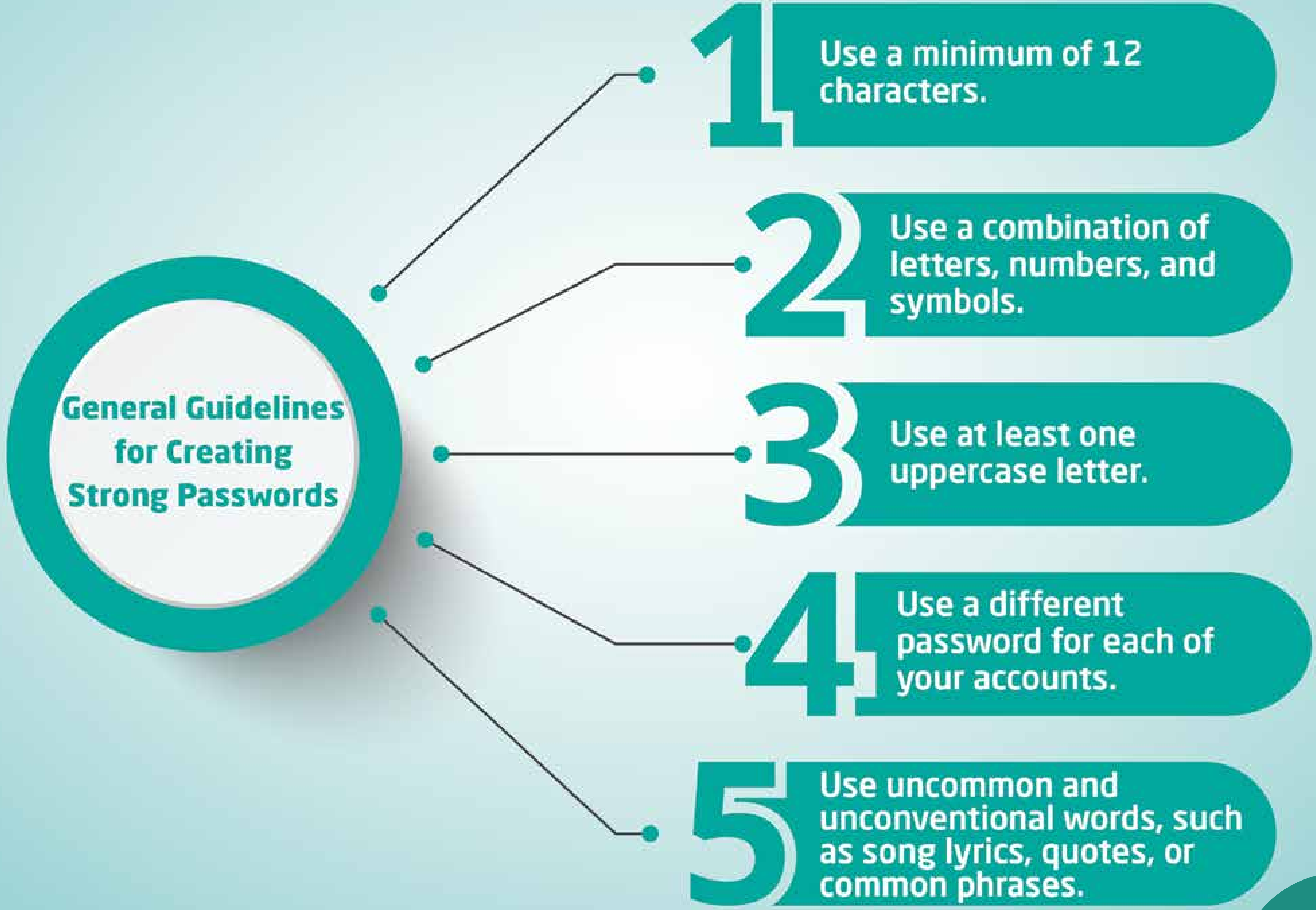
Run a scan using your new program.

3

Change all your passwords.

The Significance of Password Protection

It serves as the first line of defense against unauthorized access to accounts, devices, and files online. Strong passwords help secure data from malicious entities and malware. The stronger the password, the greater the protection of information.



General Guidelines for Creating Strong Passwords

1. Use a minimum of 12 characters.
2. Use a combination of letters, numbers, and symbols.
3. Use at least one uppercase letter.
4. Use a different password for each of your accounts.
5. Use uncommon and unconventional words, such as song lyrics, quotes, or common phrases.

References

Arabic references:

1. Ibrahim, Hammadi Othman. Information Security, Computer Lectures, Department of English Language, College of Education for Human Sciences, Al-Anbaa University, Iraq. Available at the link: https://www.uoanbar.edu.iq/eStoreImages/Bank/1352. pdf.

2. Ransomware - definition, prevention and removal, Kaspersky. Available at the link: HTTPs://cutt.us/G5L3h.

3. Al-Shamekh, Iman. Millions in losses... How did ransom viruses set fire to the world of technology? May 2023 AD, Al Jazeera. Available at the link: https://cutt.us/2szL7.

4. Al-Akaila, Abdullah Majid Abdul Muttalib. Theft of electronic data and information "A comparative study", College of Sciences and Humanities - Department of Law, Prince Sattam bin Abdulaziz University. Available at the link: https://jfslt.journals.ekb.eg/article_10943_869bcc9f604774fe726ffe0bc9e5878b.pdf.

5. How to protect your device from malware, salamatechwiki. Available at: https://cutt.us/ssynj.

6. What is meant by malware? support.google.com. Available at: https://support.google.com/google-ads/answer/2375413?hl=ar.

7. Mosli, Tariq. 7 security threats when using public Wi-Fi: (and how to protect yourself from them), Information Security, 2021 AD, available at the link https://cutt.us/cb7w0

English references

1. 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe. On Site: https://www.digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-online-safe.

2. Broken cryptography, resources. On site: https://cutt.us/an1BC.

3. Detecting and Responding to Unauthorized Access. Top 8 Practices to Implement, June 28, 2023. On Site: https://www.ekransystem.com/en/blog/detecting-and-responding-to-unauthorized-access.

4. How Ransomware Works, unitrends. On Site: https://www.unitrends.com/solutions/ransomware-education.

5. Kyle Chinj How to Back Up Your Data: 6 Effective Strategies to Prevent Data Loss, 2023. On Site: https://www.upguard.com/blog/how-to-back-up-your-data.

6. Malware, malwarebytes. On Site: https://www.malwarebytes.com/malware.

7. Mitigating malware and ransomware attacks, how to defend organisations against malware or ransomware attacks. On Site: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

8. Mobile Cyber Threats, Kaspersky Lab&Interpol Joint Report. On site: https://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf.

9. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97–106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088.

10. O. V. Syuntyurenko & R. S. Gilyarevskii. Trends and Risks of Network Technologies, , Scientific and Technical Information Processing volume 48, pages97–106 (2021). On site: https://link.springer.com/article/10.3103/S0147688221020088

11. The 12 Most Common Types of Malware, Kurt Baker - February 28, 2023. On Site: https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/.

12. The 5 most common types of data stolen, Lewis Morgan, March 2014. On Site: https://www.itgovernance.co.uk/blog/the-5-most-common-types-of-data-stolen.

13. Top Trends and Threats in Mobile Security: Gartner, cxotoday. On site: https://cutt.us/oMMsw.

14. What do I do to protect against Ransomware? security.berkeley.edu. On Site: https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware.

15. What is data theft and how to prevent it, Kaspersky. On Site: https://www.kaspersky.com/resource-center/threats/data-theft.

16. What Is Network Security? cisco. On site: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

17. What is password protection? Microsoft. On Site: https://www.microsoft.com/en-us/security/business/security-101/what-is-password-protection

18. What is Ransomware? checkpoint. On Site: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/.

19. What is unauthorized access? nordvpn. On Site: https://nordvpn.com/blog/unauthorized-access/.

CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency