BACK 2
BASICS

SECURITY

A CYBERSECURITY HANDBOOK

universidade
de aveiro

Co-funded by
the European Union

Disclaimer: 2021-1-PT01-KA220-HED-000023543
This project has been funded with support from the European Commission. This publication and all its contents reflect the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

BACK 2
BASICS

A CYBERSECURITY HANDBOOK

A comprehensive guide to cybersecurity best practices that empowers individuals and organizations to protect against common threats in the digital world.

universidade
de aveiro

BIO
LIVING

HELLENIC
REPUBLIC
UNIVERSITY
OF MACEDONIA

gri

Title
SECURITY - A Cybersecurity Handbook

Project
Back2Basics - Bridging the gap between higher education and labour market by fostering digital skills

Project reference
Erasmus+ 2021-1-PT01-KA220-HED-000023543

Coordination
João Rafael Almeida [Cybersecurity Office of the University of Aveiro]
Cristina Cerqueira [Cybersecurity Office of the University of Aveiro]
João Paulo Barraca [Cybersecurity Office of the University of Aveiro]
Rita Santos [Communication and Art Department/Digimedia, University of Aveiro]

Contributs | Partners (in alphabetic order)
Associação Bioliving
GRI — Gabinete de Recolocación Industrial
University of Aveiro
University of Macedonia

Graphic Design
Gonçalo Gomes [Communication and Art Department/ID+, University of Aveiro]

Illustrations
Vectorjuice / Freepik

Publisher
UA Editora
University of Aveiro

ISBN
978-972-789-926-5

DOI
https://doi.org/10.48528/kc3g-e490

SUMMARY

In an increasingly interconnected world, cybersecurity is of paramount importance. This handbook serves as a valuable resource for individuals and organizations seeking to navigate the ever-evolving landscape of cyber threats. Covering topics ranging from social engineering and phishing to malware prevention and multi-factor authentication, this comprehensive guide provides practical advice and best practices to mitigate risks. This handbook empowers readers to protect their digital assets and maintain a secure online presence by promoting cybersecurity awareness, emphasizing the importance of proactive measures, and offering guidance on maintaining robust defenses. Whether you are an individual concerned about personal security or an organization looking to enhance your cybersecurity protocols, this handbook equips you with the knowledge and tools necessary to navigate the digital realm safely and confidently.

BACK 2 BASICS

1 A CYBERSECURITY HANDBOOK INTRODUCTION

INTRODUCTION

In today's interconnected world, where technology has become an integral part of our daily lives, the importance of cybersecurity cannot be overstated. In this way, this was one of the essential competences considered in the “Back2Basics - Bridging the gap between higher education and labour market by fostering digital skills”, Erasmus + project (2021-1-PT01-KA220-HED-000023543), which aims at addressing digital transformation in the HE system and bringing Higher Education systems and labour markets closer together, working in the enhancement of digital skills.

This comprehensive handbook is designed to give individuals the fundamental knowledge required to navigate the constantly evolving landscape of cyber threats while safeguarding against potential risks. Although the digital age has brought tremendous benefits, it has also exposed our information to a wide range of potential issues that can result in severe consequences. By understanding these issues, individuals can

better recognize the importance of cybersecurity in their personal and professional lives.

The insidious rise of social engineering attacks highlights the increasing sophistication of cybercriminals, who employ psychological tactics to manipulate unsuspecting individuals into divulging sensitive information or engaging in actions that compromise their security – phishing emails being a prime example of this strategy. Phishing involves fraudulent emails or websites designed to deceive individuals into sharing personal information, such as passwords or credit card details. Falling victim to such attacks can lead to financial loss, identity theft, and reputational damage. Moreover, the prevalence of malware poses a significant threat to individuals and organizations alike. Malware is software designed for malicious purposes. This type of software can infect computers or networks, and compromise data security and system integrity. For example, ransomware is a type of malware that encrypts valuable files on the target machine and demands a ransom for their release. Organizations of all sizes have fallen victim to such attacks, resulting in financial losses, operational disruptions, and damage to their reputation.

One of the primary objectives of this handbook is to raise awareness about the significance of cybersecurity for the public in general. It will delve into various topics, including social engineering, phishing, malware prevention, password management, multi-factor authentication, and more. It will provide practical advice, best practices, and real-world examples to empower readers to safeguard their digital lives and mitigate the risks associated with cyber threats. In the subsequent chapters, some of the proactive measures and strategies that can be employed to stay secure in the digital world are explored. By developing a strong foundation in cybersecurity awareness and adopting effective defensive practices, individuals can collectively build a safer and more resilient digital environment for everyone.

BACK 2
BASICS

2 A CYBERSECURITY HANDBOOK COMMON THREATS

COMMON THREATS

The context of a threat in cybersecurity should be viewed as a potential precursor to an undesired incident that can result in damage to data, systems, individuals, or organizations. This section provides an overview of common threats for individuals.

SOCIAL ENGINEERING

Social engineering goes beyond a deceptive tactic used by cybercriminals to manipulate individuals into disclosing sensitive information or performing actions that may compromise their security. This technique is not limited to cyberspace and can occur outside of it, aiming to gather privileged information about a specific system, which may help attackers to succeed. It capitalizes on human psychology and exploits our inherent tendencies, such as, trust, curiosity, or the desire to help others. Why is this important? Social engineering aims to

prompt individuals to make decisions without much thought about what is happening, which can be advantageous for attackers exploiting vulnerabilities in those processes. Ultimately, the main goal is to compel a target to take a specific action without thoughtful consideration. The more people reflect on the actions they are taking, the more likely they are to recognize that these actions are part of a manipulation.

For instance, consider a TV commercial featuring a famous female artist. The commercial begins in a gloomy setting with a somber song, portraying the artist amidst a depressing environment. The scene then shifts to a different location where puppies appear distressed and undernourished, evoking a sense of despair. The artist explains that without our donations the puppies won´t survive. Following these poignant scenes, the artist reappears, now joyful and surrounded by healthy dogs accompanied by an enthusiastic song. What is the underlying message? The commercial suggests that, for a small donation, the plight of these poor animals can be transformed, and they can share their love with the audience. Although the intention may not be selfish, nonetheless, this commercial aims to manipulate the emotions of the audience, eliciting positive feelings when people contribute to saving the puppies.

The same principle can be applied for malicious purposes. In a hypothetical situation where an attacker wants to access a specific company, this individual can manipulate the attention of the receptionist to bypass the first human barrier. Examples of such strategies might include creating a sense of urgency, such as claiming an urgent need for maintenance in a specific part of the building. Although this example may seem trivial, it is important to acknowledge that social engineering is not confined to cyberspace.

Cybercriminals meticulously design their attacks to appear legitimate, exploiting common human vulnerabilities to achieve their malicious goals. Within the cyberspace, these attacks can take various forms, such as phishing, pretexting, baiting, or even physical manipulation. The success of social engineering attacks often relies on creating a sense of urgency, exploiting trust, or leveraging emotional triggers. For instance, an attacker might craft an email posing as a bank representative, alleging that the recipient's account has been compromised and urging them to click on a link to resolve the issue. These tactics manipulate individuals into acting without critically evaluating the situation, bypassing their normal skepticism.

To safeguard against social engineering attacks, individuals should remain vigilant and develop a healthy skepticism when engaging with any form of communication. It is essential to verify the authenticity of requests, particularly if they involve sensitive information or unexpected actions. This verification can be achieved by independently contacting the organization or person through a trusted communication channel to confirm the legitimacy of the request. By adopting a cautious approach and staying informed about the latest social engineering techniques, individuals can enhance their ability to protect themselves against these deceptive tactics.

PHISHING, VISHING AND SMISHING

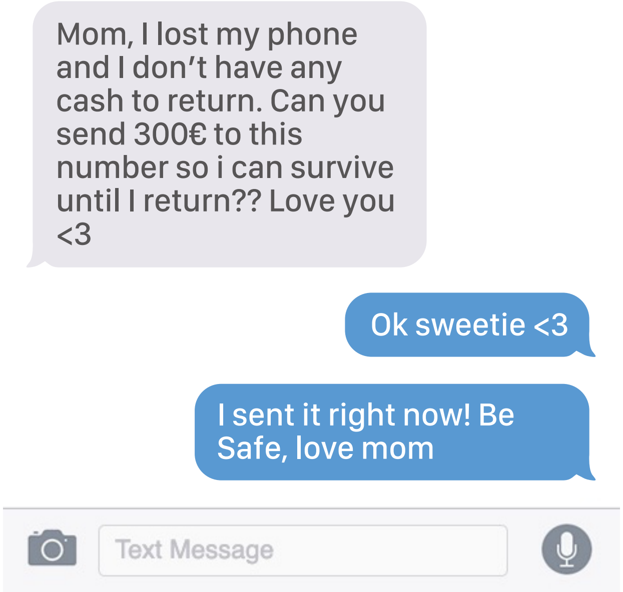
One common form of social engineering is phishing, where attackers send fraudulent emails that appear to come from reputable organizations or individuals. These messages often contain urgent requests, enticing offers, or alarming alerts, aiming to prompt recipients into taking immediate action. They may ask for sensitive information like passwords, credit card numbers, or login credentials under the guise of a legitimate need. These attacks manifest in various forms, including email phishing, smishing (SMS-based phishing) and voice phishing (vishing). Email phishing is the most common type, with attackers sending emails that appear genuine, often using official logos, language, and design elements to deceive recipients. Smishing and vishing employ similar tactics but through text messages or phone calls, respectively.

The goal of such attacks can be broken down into various aims:

- **Delivering malicious payloads - the part of a malicious software that executes malicious actions - that provide remote access to attackers;**
- **Stealing the victim's credentials;**
- **Collecting other information that can be used to scale another attack.**

In addition to these generic messages that reach a broad audience, there is a more personalized technique known as spear phishing. This method requires some preparation from the attackers' perspective, as they need to acquire information about the victim. Typically, they use something very personal that is publicly available online and easily accessible to anyone. This information often originates from posts on social networks, sometimes published unwittingly by the victim´s relatives, among others.

For instance, consider a group of friends setting out on a week-long vacation. During this trip, it is normal to publish several photos across various social networks. If an attacker is monitoring this group online and possesses additional information about their relatives, they can use this knowledge to contact the parents of one of the friends. At this point, the attacker might use a dummy phone or profile to initiate contact with the following context:



Mom, I lost my phone and I don't have any cash to return. Can you send 300€ to this number so i can survive until I return?? Love you <3

Ok sweetie <3

I sent it right now! Be Safe, love mom

The expected action from the parents would be to double-check before sending any money. However, certain elements of the story made sense, creating a perfect scenario for falling victim to spear phishing. Our daily lives are full of similar examples, instances where individuals act impulsively without thorough consideration.

To avoid falling victim to phishing attacks, it is essential to remain vigilant and adopt preventive measures. In the case of emails, individuals should first scrutinize the sender's email address, being wary of any discrepancies or unfamiliar domains that do not match the purported organization. Next, they should carefully evaluate the content of the email, paying attention to spelling or grammar errors, generic salutations, or urgent requests designed to create a sense of panic. Legitimate organizations typically address individuals by name and provide clear and concise information. Finally, individuals should avoid clicking on suspicious links or downloading attachments without verifying their legitimacy. Incorporating these practices will enhance personal resilience against these schemes. A strategy to identify malicious links is to hover over the link to reveal their actual destination, ensuring they lead to legitimate websites. Individuals should exercise caution if the link redirects to an unfamiliar or suspicious URL. Additionally, it is advised to type URLs directly into the browser or use bookmarks to access trusted websites.

Furthermore, install and regularly update reputable security software, such as antivirus or anti-malware programs, to detect and block potential phishing attempts. Educating yourself about phishing techniques is also crucial for recognizing and avoiding these attacks. Stay informed about the latest phishing trends, common red flags, and emerging tactics employed by cybercriminals.

THE SILENT INVADERS: AN OVERVIEW OF THE DIFFERENT TYPES OF MALWARE

Malware refers to any software specifically designed to harm or exploit computer systems, networks, or individuals. It encompasses a wide range of malicious programs, including viruses, worms, trojans, spyware, and ransomware. Malware can be distributed through various means, such as infected email attachments, compromised websites, or malicious downloads. Once installed, malware can compromise data, steal personal information, disrupt system operations, or provide unauthorized access to cybercriminals. Understanding the diverse types of malwares is crucial in building effective defense strategies. Below we briefly describe the different categories of malware:

- **Viruses:** These digital parasites infiltrate host files, spreading their code when the infected file is executed. Much like biological viruses, computer viruses replicate themselves, often causing damage and chaos in their wake.

- **Worms:** Unlike viruses, worms operate independently and spread across networks, exploiting vulnerabilities to propagate. Their self-replicating nature allows them to rapidly infect multiple systems.

- **Trojans:** Named after the legendary Greek deception, Trojans masquerade as legitimate software, deceiving users into willingly inviting them in. Once inside, they pave the way for unauthorized access and control.

- **Spyware:** Operating in the shadows, spyware silently collects sensitive information, from passwords to personal data, often for the purpose of espionage or identity theft.

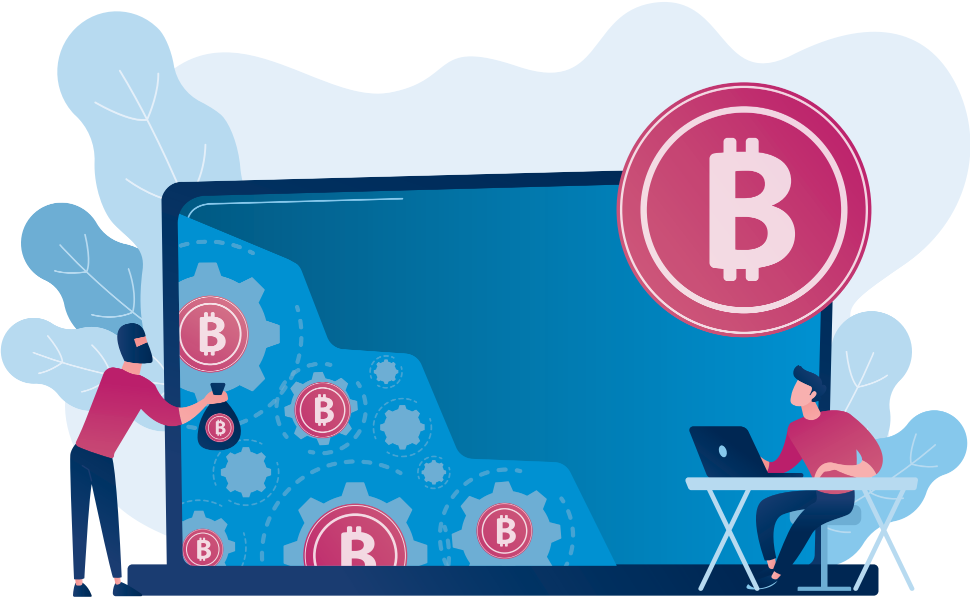
- **Adware:** While less sinister, adware bombards users with unwanted advertisements, impacting system performance and user experience. It often serves as a vehicle for generating revenue for cybercriminals.

- **Rootkits:** Stealthy and evasive, rootkits delve deep into a system's core, providing persistent access and control to malicious actors. They are notoriously difficult to detect and remove.

- **Keyloggers:** These surreptitious tools track and record keystrokes, capturing sensitive information such as passwords and credit card details, enabling cybercriminals to steal valuable data.

- **Ransomware:** This is a specific type of malware that encrypts the victim's files, rendering them inaccessible until a ransom is paid. Typically, it infiltrates systems through phishing emails, malicious attachments, or exploit kits. Once activated, ransomware encrypts important files and displays a ransom note demanding payment in exchange for the decryption key. Ransomware attacks have become increasingly sophisticated, targeting individuals, businesses, and even critical infrastructure.

In the past, malware was developed with several vulnerabilities, which helped cybersecurity professionals reverse the damages caused. However, in recent times, cybercriminals have improved the "quality" of their applications by using algorithms known for their high resistance to decryption. This creates a particularly challenging scenario since on a common computer it would take billions, or even trillions, of years to recover the key to decrypt the files. Although paying the ransom might seem reasonable, especially when you consider the impact of the lost information, it is often the worst decision for several reasons. First, the individual who pays the ransom indirectly signals to the attacker that they are an excellent target because payment is guaranteed. In other words, it is like placing a cyber target on that person. Second, and no less significant, is the lack of assurance that the provided key will decrypt the files. Who can guarantee that the attacker will act honestly?



The impact of malware extends beyond individual systems, sending ripples across personal, business, and governmental landscapes.

- **Financial loss:** Incidents related to malware can result in substantial financial losses, including ransom payments, recovery costs, and potential legal penalties.
- **Data breaches:** Malware compromises sensitive data, jeopardizing personal privacy and corporate confidentiality. The aftermath of data breaches can be long-lasting and irreparable.
- **Operational disruption:** Ransomware attacks can cripple operations, causing downtime and affecting productivity on a massive scale.
- **Reputational damage:** Organizations affected by malware incidents often suffer reputational damage, eroding customer trust and confidence.
- **National security concerns:** State-sponsored malware campaigns raise significant national security concerns, targeting critical infrastructure and governmental institutions.

In the vast and intricate landscape of cybersecurity, malware emerges as a formidable adversary. Its diverse forms and insidious impact serve as a constant reminder of the digital threats we face in our interconnected world. By understanding the multifaceted nature of malware, we can better comprehend the necessity for robust cybersecurity measures and ongoing vigilance. As technology continues to evolve, the battle against malware remains a pivotal aspect in safeguarding our digital future.

UNMASKING MISLEADING WEBSITES AND FAKE NEWS

In an era characterized by the unprecedented accessibility of information, a sinister underbelly has emerged within the digital landscape – misleading websites and the pervasive spread of fake news. As we traverse the intricate pathways of the internet, it becomes increasingly crucial to navigate these treacherous waters with vigilance. Diving deep into the world of misleading websites and uncovering the unsettling effects of fake news, we can describe key points about where they come from, how they work, and the wide-ranging impact they have.

In the realm of misleading websites, the illusion of legitimacy is masterfully woven through various tactics. These deceptive platforms often use sophisticated design and mimicry to emulate genuine sources, blurring the lines between authenticity and deception. Subtle manipulation comes into play, leveraging persuasive language and misleading imagery to exploit cognitive biases, enticing users to consume and share content without a second thought. Feigned authority further adds to the illusion, as misleading websites manufacture endorsements and testimonials, creating an outer veneer of credibility that easily entraps unsuspecting readers. Within this intricate web of deceit, a thriving ecosystem of fictitious information arises. These platforms skillfully present a concoction of both authentic and fabricated data, resulting in a distortion of reality that sow seeds of confusion among an unsuspecting audience.

With malicious intent at its core, the dissemination of fake news often operates as a tool for misleading, manipulating, or swaying public opinion to further specific agendas or ideologies. Fueled by technological catalysts, the rapid dissemination of fake news is intensified through the virality of social media and

algorithmic amplification. This dynamic allows misinformation to permeate vast audiences in unprecedented timeframes. The corrosive effect extends to the erosion of trust, as repeated exposure to fake news erodes public confidence in established institutions, cultivating an atmosphere of skepticism that could potentially diminish the credibility of factual reporting. The influence of fake news doesn't stop there, it extends to shaping individual beliefs and collective decision-making processes, underscoring the urgency of countering its insidious impact. The global ramifications are undeniable as fake news transcends borders, exerting its influence on international relations, shaping public health responses, and inflaming societal tensions with far-reaching consequences.

The impact of misleading websites and fake news extends far beyond the realm of the digital landscape, leaving an indelible mark on various aspects of society. The influence of fake news on public discourse and individual beliefs can lead to the erosion of trust in established institutions, creating an environment of skepticism that undermines the very foundations of a well-informed citizenry. Misleading websites, with their artful mimicry of legitimacy, contribute to this erosion by blurring the lines between fact and fiction, leaving individuals vulnerable to manipulation. These are fundamental to supporting other attacks, such as phishing. Moreover, the rapid dissemination of false information through social media amplifies the impact, as sensationalized stories and deceptive narratives spread like wildfire, potentially inciting unrest and exacerbating societal tensions. As a result, the profound implications of fake news and misleading websites stretch into domains such as political discourse, social cohesion, and public health, underscoring the urgent need for media literacy, critical thinking, and responsible digital engagement to navigate this complex and evolving landscape.

BACK 2
BASICS

3

A CYBERSECURITY HANDBOOK

CYBER-HYGIENE: BEST PRACTICES

CYBER-HYGIENE: BEST PRACTICES

In today's digitally driven world, where our lives are intertwined with technology in unprecedented ways, the concept of cyber-hygiene has emerged as a critical cornerstone of responsible and secure online behavior. Just as we prioritize personal hygiene to maintain our physical well-being, adopting robust cyber-hygiene practices is essential for preserving our digital health and safeguarding against a rapidly evolving landscape of cyber threats. This section of the document delves into the realm of cyber-hygiene, illuminating a comprehensive array of best practices that empower individuals to navigate the digital realm with confidence, resilience, and heightened awareness of the cybersecurity landscape. From fortifying passwords to cultivating a discerning eye for phishing attempts, this chapter serves as a guide to elevate your digital well-being and foster a safer, more secure online experience.

DEFINING CYBER-HYGIENE

In an increasingly interconnected world, where our lives are intertwined with technology, it has become essential to prioritize cybersecurity. Just as we practice personal hygiene to protect our physical well-being, adopting good cyber-hygiene habits is crucial to safeguard our digital lives. But what exactly is cyber-hygiene?

Cyber-hygiene refers to a set of best practices and habits that individuals and organizations should adopt to ensure the security and integrity of their digital environment. It encompasses a wide range of actions and behaviors that contribute to preventing cyber threats, such as malware infections, data breaches, and identity theft.

Being cyber-hygienic is of utmost importance in today's digital landscape. Cyber threats continue to evolve and grow in sophistication, posing significant risks to individuals and organizations alike. By practicing good cyber-hygiene, we can proactively protect ourselves and our sensitive information from malicious actors. It helps prevent potential consequences such as identity theft, financial loss, and reputational damage. Maintaining strong passwords, regularly updating software, and being cautious of phishing attempts are just a few examples of cyber-hygiene practices that can significantly reduce the likelihood of falling victim to cyberattacks. Moreover, being cyber-hygienic not only safeguards our own digital well-being but also contributes to the collective security of the interconnected world, fostering a safer online environment for everyone.

RECOMMENDATIONS FOR STAYING SAFE ONLINE

Regularly updating your software is akin to tending a digital garden. Operating systems, applications, and security software evolve to address newfound vulnerabilities and enhance protection. An up-to-date system is your frontline defense against cyber threats, ensuring that potential entry points for hackers are sealed shut. By enabling automatic updates or consistently checking for updates, you proactively thwart the attempts of cybercriminals to exploit outdated software, safeguarding your digital garden. Embracing the practice of software updates is a powerful stride towards a more secure digital existence. With each update, you empower your devices with the latest security patches, making it exponentially tougher for cyber attackers to breach your defenses. These updates don't just repel imminent threats - they cultivate a proactive mindset that bolsters your cybersecurity resilience. By allotting a few minutes to regular updates, you contribute to a safer online environment for yourself and others, demonstrating the potency of collective vigilance.

In the realm of cybersecurity, a robust password is the user’s virtual fortress, guarding against unauthorized access. Crafting a strong password is not a mere task, it is an art. By intertwining a symphony of letters, numbers, symbols, and cases, it is possible to compose a passphrase that is both formidable and difficult to crack. Each account deserves its own passphrase. Consider enlisting the aid of a trustworthy password manager, relieving users from the mental burden of recalling intricate codes and ensuring that your digital keys remain securely stored. More details about this topic are discussed in the following sections.

Amidst the digital currents, phishing scams are the deceptive whirlpools that seek to ensnare unsuspecting victims. Vigilance is your compass; before succumbing to an email´s enticing lure, scrutinize its authenticity. Hovering over links to discern their true destination is a small yet potent act that can safeguard you from the precipice of a potential breach. When an email invokes urgency, pause and exercise caution. This is the modus operandi of cyber tricksters seeking to capitalize on hasty decisions. Trust your instincts and verify the sender's identity through established communication channels, deterring the cunning bait of a phishing expedition. Skepticism, coupled with

critical thinking, form an indomitable shield against the treacherous tide of phishing attempts. Think of yourself as a cyber-detective investigating clues and piecing together the truth. By embracing a vigilant and cautious mindset online you transform into an adept navigator, navigating the treacherous waters of deception with unwavering discernment. Remember, a moment of skepticism can prevent hours of damage control, illustrating the potency of a vigilant and discerning mindset.

Public Wi-Fi networks offer the allure of seamless connectivity, yet they often conceal hidden risks. Engaging with these networks demands a cautious approach; treat them like crowded marketplaces where personal information is on display. Activities involving sensitive data, such as online banking or transferring confidential documents, should be reserved for secure, private connections. The judicious use of a Virtual Private Network (VPN) acts as a digital cloak, encrypting your data and shielding it from prying eyes, rendering you impervious to potential eavesdroppers. In the realm of network safety, awareness and prudence are your guiding stars. Consider public Wi-Fi networks as bustling squares teeming with strangers, where your secrets could be overheard by any passerby. The digital mask of a VPN adds an extra layer of protection, ensuring that your digital footprint remains shrouded from curious onlookers. By adopting these practices, you empower yourself with the tools to roam the virtual world with confidence, knowing that your online activities are safeguarded against potential adversaries.

While the aforementioned strategies contribute to increased online safety, let´s delve into a comprehensive list of the top ten best practices to foster resilience against cyber threats.

1. **Strong passwords:** Create unique, strong passwords for each account.
2. **Multi-Factor Authentication (MFA):** Use MFA whenever available.
3. **Regular updates:** Keep software and devices up to date.
4. **Be cautious online:** Watch for suspicious emails and links.

5. **Avoid public Wi-Fi:** Avoid sensitive activities on public Wi-Fi.
6. **Backup data:** Regularly back up important files.
7. **Privacy settings:** Adjust social media privacy settings.
8. **Secure devices:** Lock devices with strong passwords.
9. **Think before you click:** Be cautious with downloads and links.
10. **Stay educated:** Stay informed about cybersecurity threats.

MITIGATION AND RECOVERY

Cyber-attacks have become a prevalent and sophisticated form of cybercrime, causing significant damage to organizations worldwide. To minimize their impact and effectively recover from such incidents, it is crucial to follow a well-defined set of guidelines. Some of the best practices for implementing a robust backup strategy to protect your valuable data can be the following:

- **Immediate isolation:** The first step in containing an attack, for example a ransomware attack, is to disconnect all infected devices, such as computers, laptops, or tablets, from any network connections, including wired, wireless, and mobile. In severe cases, consider turning off Wi-Fi, disabling core network connections, and disconnecting from the internet if necessary.

- **Reset credentials:** Resetting credentials, especially passwords for administrator and system accounts, is crucial to prevent further unauthorized access. However, exercise caution to avoid locking yourself out of essential systems required for recovery.

- **Safely wipe infected devices:** In the case of malware attacks, to eradicate the issue completely safely wipe infected devices and reinstall the operating system. This step ensures that any remnants of the malware are removed, providing a clean slate for recovery.

- **Verify backup integrity:** Before restoring from a backup, ensure that it is free from any malware. Only proceed with the restoration process if you are confident that both the backup and the device where you´re installing it are clean.

- **Connect to a clean network:** To download, install, and update the operating system and all other software, connect the devices to a clean network. This ensures that no infected files are inadvertently transferred during the recovery process.

- **Install and update antivirus software:** Protect your systems from future attacks by installing, updating, and running reliable antivirus software. Regularly scanning your devices with the latest antivirus definitions can help identify and eliminate any remaining infections.

- **Network reconnection:** Once you have taken the necessary precautions and ensured the integrity of your systems, reconnect to your network. However, closely monitor network traffic and conduct periodic antivirus scans to detect any signs of lingering malware.

DESIGNING A ROBUST BACKUP STRATEGY

The best solution for enhancing security in cyberspace is anticipating potential problems. To be prepared for cyber threats, it is recommended to use backups, specifically by implementing a strong backup policy that emphasizes regular backups for critical files. The importance of these files may vary for each user or organization, so it is essential to assess and prioritize your specific needs. The recommendations are as follows:

- **Offline and Offsite Backups:** To protect your backups from attacks, create offline backups stored in a different location, preferably offsite. Consider using cloud storage services explicitly designed for secure backups. Diversify backup solutions and storage locations to minimize the risk of data loss. Adhering to the 3-2-1 backup strategy ensures redundancy and resiliency.

- **Disconnect Backup Devices:** Avoid keeping external hard drives containing backups permanently connected to your network. In the case of an attack, if these devices are connected, they may become affected. For instance, ransomware operators often target connected backup devices, making data recovery more challenging. Disconnecting them when not in use mitigates this risk.

- **Protect Previous Versions:** Ensure that your chosen cloud service provider safeguards previous versions of backups. Some services automatically synchronize files, potentially replacing unencrypted versions with encrypted copies. Maintaining multiple versions of backups ensures the availability of uncorrupted data for recovery.

- **Regularly Patch Backup Servers:** Patch your backup servers regularly to address any vulnerabilities that could be exploited by attackers. Proactively identifying and fixing weaknesses may enhance the security and resilience of your backup infrastructure.

- **Verify Clean Devices:** Before initiating the restoration process, ensure that your backups are only connected to known clean devices. Additionally, scan backup solutions for malware to prevent inadvertently reintroducing infected files into your network.

By following the recommended guidelines and implementing a robust backup strategy, you can significantly minimize the impact of a ransomware outbreak and ensure a swift and effective recovery process. Regularly updating and testing data backups and recovery procedures is crucial to ensure that, in the evento of a cyberattack, they will effectively recover your data and minimize downtime.

BACK 2 BASICS

4

A CYBERSECURITY HANDBOOK

PASSWORD MANAGEMENT AND SELF-PROTECTION

PASSWORD MANAGEMENT AND SELF-PROTECTION

Effective password management is a fundamental aspect of self-protection in the digital landscape. It encompasses not only creating strong, unique passwords, but also their diligent management and regular review. This entails employing strategies like utilizing a reliable password manager to store and organize different passwords, ensuring that each account has a distinct password to prevent a breach in one account from compromising other accounts. Regularly updating passwords, particularly for sensitive accounts and being vigilant about potential phishing attacks are equally crucial. Self-protection extends to being aware of the security features provided by different platforms, such as two-factor authentication, which adds an additional layer of security. Equally important is the awareness of one's digital footprint and the potential risks involved in sharing personal information online. By staying informed and adopting robust password management practices, individuals can significantly enhance their online security and protect their personal and sensitive information from unauthorized access.

RISKS OF WEAK PASSWORDS

Before defining what weak passwords are and the impact of their weakness, we first need to understand how attackers can crack our credentials. There are different ways to obtain an individual´s credentials, assuming that these were not provided in a phishing attack. An attacker can intercept communication, performing what is known as a Man-In-the-Middle attack. With the popularization of HTTPS communications, these attacks have become less effective, therefore we will not discuss them further in this document. However, another technique is stealing databases by exploiting existing vulnerabilities in web applications.

This last issue is still a concern and is complex to control. When an attacker succeeds in stealing a private database containing credentials, these are stored in three ways:

1. **as free text (less common in current days);**
2. **using a hash, which is a technique that converts the password into something different using irreversible algorithms; and**
3. **using a hash with salt, which is more robust.**

The process of hashing a password is based on digest functions. The goal of these functions is the creation of a defined set of bits that represent the original information. These follow some principles, one of which defines that using a hash should not be possible to obtain the original information that created

such a hash. Therefore, an attacker who has a hash of a password is not able to obtain the password directly.

The initial hashes were designed to be secure, but later discoveries revealed certain techniques capable of breaking some hashes almost instantaneously. This led to the development of more advanced and secure hashing algorithms. The vulnerability of passwords is most commonly exposed in scenarios such as:

- **Stored in Compromised Databases:** When passwords are stored in databases that are not adequately secured, they become susceptible to unauthorized access and potential breaches.

- **Stored in Clear Text:** Storing passwords in clear text, without any form of encryption, makes them easy targets for cybercriminals who gain access to the storage system.

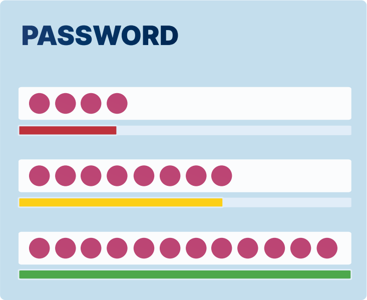
- **Represented Using Hashes:** While hashes are used for added security, certain hashing algorithms have been found vulnerable, making passwords susceptible to attacks.

- **Intercepted in Communication:** Passwords can be intercepted during their transmission over networks, especially if the communication channel is not securely encrypted.

- **Unprotected Networks:** Using passwords on unprotected or public networks increases the risk of them being captured by malicious actors, as these networks often lack sufficient security measures.

Understanding these common vulnerabilities underscores the importance of robust password management and security practices in safeguarding personal and sensitive information.

DEFINING STRONG PASSWORDS



Defining strong passwords is crucial for protecting your online accounts and personal information. Here are some key guidelines for creating strong passwords:

- **Length Matters:** Aim for at least 12 to 16 characters. Longer passwords are generally more secure.
- **Use a Mix of Characters:** Incorporate a variety of characters in your password, including:
  - **Uppercase letters (A-Z)**
  - **Lowercase letters (a-z)**
  - **Numbers (0-9)**
  - **Special characters (e.g., !, @, #, $)**
- **Avoid Predictable Patterns:** Don't use sequential or repetitive characters (like "12345" or "aaaaa"). These are easier for attackers to guess.
- **No Personal Information:** Avoid using easily guessable information such as your name, birth date, or common words. These can often be found on social media or guessed.
- **Uncommon Words or Phrases:** Consider using a random, uncommon word or phrase. Even better, string together several unrelated words.
- **Consider a Passphrase:** A passphrase is a sequence of words or a

sentence. It's easier to remember and can be quite long, making it more secure. For instance, "BlueCoffeeMugOnDesk!".

- **Use Non-Standard Substitutions:** If you do use words or phrases, try creative substitutions, like using a "3" for an "E" or a "$" for an "S".
- **Test Your Password:** Many online tools allow you to check the strength of your password (tip: don´t use your actual password). They can give you a sense of how easy or difficult it would be to crack.
- **Change Passwords Regularly:** While not always necessary, especially if you use a unique and strong password, changing passwords regularly can be beneficial, particularly for sensitive accounts.
- **Stay Informed:** Be aware of current best practices for password security, as recommendations can evolve with changing technology and security threats.

By following these guidelines, you can create strong, effective passwords that help protect your digital information. Remember, the strength of a password often lies not just in its complexity, but also in its uniqueness and unpredictability.

RECOMMENDATIONS FOR MANAGING PASSWORDS

Managing passwords effectively is crucial for maintaining online security and privacy. Here are some recommendations for managing passwords:

- **Use Strong and Unique Passwords:** Each of your accounts should have a unique password. Strong passwords typically include a mix

of letters (both uppercase and lowercase), numbers, and special characters. Avoid common words and phrases.

- **Employ a Password Manager: P**assword managers can generate and store complex passwords for you. They keep your passwords secure and accessible through one master password. This reduces the burden of remembering multiple strong passwords.

- **Two-Factor Authentication (2FA):** Whenever possible, enable 2FA. This adds an extra layer of security by requiring a second form of identification beyond just your password, such as a text message code or an app notification.

- **Regularly Update Passwords:** Change your passwords regularly, especially for sensitive accounts like email, banking, and social media. However, frequent changes aren't necessary if you use strong, unique passwords and have not experienced a breach.

- **Beware of Phishing Attacks:** Be cautious about where you enter your password. Phishing attacks often lure individuals into providing their passwords on fake websites. Always verify the website's URL before entering your credentials.

- **Security Questions:** Choose security questions and answers that aren't easily guessable. Sometimes, information like your mother's maiden name or your first school can be found online or guessed.
- **Monitor Accounts for Breaches:** Use services that alert you if your email or password has been compromised in a data breach. This allows you to change your password immediately.
- **Avoid Using Personal Information:** Avoid using easily accessible information like your name, birthdate, or simple sequences like "1234" in your passwords.
- **Do Not Share Passwords:** Avoid sharing your passwords with others. If you must share a password, change it as soon as possible afterwards.
- **Backup Recovery Information:** Ensure your account recovery information is up-to-date. This includes your email address or phone number used for recovering your accounts in case you forget your password.

The key to effective password management is a combination of strong, unique passwords, the use of a reliable password manager, and staying vigilant against security threats.

BACK 2
BASICS

5

A CYBERSECURITY HANDBOOK

CONCLUSION

CONCLUSION

Throughout this handbook, we have explored the critical importance of cybersecurity and delved into various best practices and strategies for protecting against common cyber threats. As we conclude our journey, let us recap the key takeaways and emphasize the significance of implementing these practices in our personal and professional lives.

First and foremost, maintaining good cyber hygiene is paramount. By regularly updating software, using strong and unique passwords, and exercising caution when connecting to public Wi-Fi networks, individuals can significantly reduce the risk of falling victim to cyber-attacks. Organizations, too, must prioritize cyber hygiene by implementing robust security measures, conducting regular security audits, and educating their employees on safe online practices.

In conclusion, the key takeaway from this handbook is that cybersecurity is a collective responsibility. By implementing the best practices discussed here, individuals and organizations can significantly reduce the risk of falling victim to cyber threats and protect their sensitive information, financial assets, and reputation. Cybersecurity is not a one-time effort but an ongoing commitment. It requires continuous education, awareness, and adaptation to stay one step ahead of cybercriminals.

Let us remember that our digital world is constantly evolving, and so are the tactics and techniques employed by cyber attackers. By remaining vigilant, staying informed about emerging threats, and adapting our defenses accordingly, we can navigate the digital landscape securely and confidently. Together, we can build a safer and more resilient digital ecosystem for the benefit of all.

universidade de aveiro

BIO LIVING

HELLENIC REPUBLIC
UNIVERSITY
OF MACEDONIA

gri