

MAKING SOCIAL CARE TECHNOLOGIES ACCESSIBLE TO ALL

Topic 1.3. Basics of online safety and cybersecurity

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of contents

Course introduction

1. Basics of cybersecurity and online safety
2. Overview of the most common threats
3. Preventive measures
4. Best practices and good habits
5. Useful tools and additional resources

Course Introduction

1. Course overview
2. Target group
3. Training objectives

Course Introduction



1. Course overview

What is the course about?

The “basics of online safety and cybersecurity” course is designed to provide social care workers with essential knowledge and skills to **protect sensitive data and ensure online safety** in the context of their work. Participants will learn how to **identify** and **mitigate** common cybersecurity risks and how to adopt **best practices** and easy-to-implement measures for online safety.

Why does it matter?

The relevance emerged of the SociALL project’s transnational research : cybersecurity is a particularly **salient and current** topic, in a context of increased cybersecurity risk, concerns about health and personal data privacy and integrity. The multiplication of cyber-attacks against **vulnerable** care organizations, as shown by the recent waves of ransomwares on European hospitals call for increased attention and knowledge.

Course Introduction



2. Target group

Who is the course for?

Virtually **any professional working in the care sector** can follow this course, as each is using digital tools daily and is, as such, exposed to cyberrisks. The course mostly consists of explanations, tips and best practices that can be applied, for most of them, individually and without important technical skills. Most of this content can serve workers in their professional life, but also apply to their personal use of digital tools.

Can I follow it?

This curriculum is adapted to **any worker** and provides rather basic, useful introduction and guidance to cybersecurity and online safety. Any person accustomed to using digital tool in their professional life is therefore able to follow, understand and learn from this course.

Course Introduction



3. Training objectives

What can I learn from the course?

- Understanding the **importance** of cybersecurity and online safety.
- Understanding the **risks** and most common **threats**
- Understanding the **human factor** in cyberattacks
- Applying **easy-to-implement measures** for data protection and online safety
- Exploiting useful **resources, tools** and globally accepted **best practices** to increase security

What will it change?

By the end of the training, participants and their organization will be able to better:

- **Mainstream** online safety in their operations
- **Identify** and **address** cybersecurity **risks**
- Change **processes** that make them **vulnerable** to more secure processes
- **Train and advise** their colleagues on the matter to create a **safer organizational culture**
- **Pass on** that knowledge to **vulnerable patients**, when **risks** are perceived by social care workers

1. Basics of cybersecurity and online safety

1. The importance of cybersecurity and online safety
2. Understanding care workers' responsibility towards patients' data integrity
3. Human errors and negligence are the main entry door for cyber criminality
4. What can we do? Identify and treat human vulnerabilities

1. Basics of cybersecurity and online safety

1.1. The importance of cybersecurity and online safety



Cybersecurity is not just a buzzword

It is a shield protecting us from various online risks, including identity theft, financial fraud, personal data theft, cyberattacks incapacitating an entire organization, etc.



Cybersecurity is a triple protection

In the care sector, cybersecurity has the role of protecting individual care workers, their organizations and their patients.



Cyberattacks are the new criminality

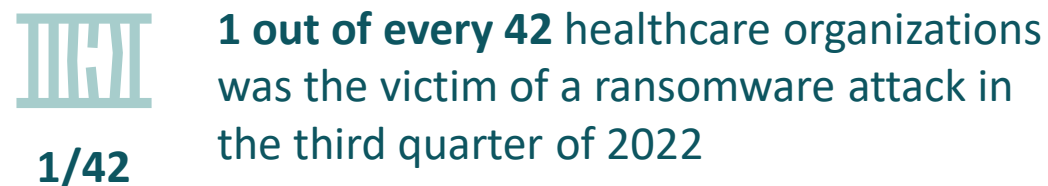
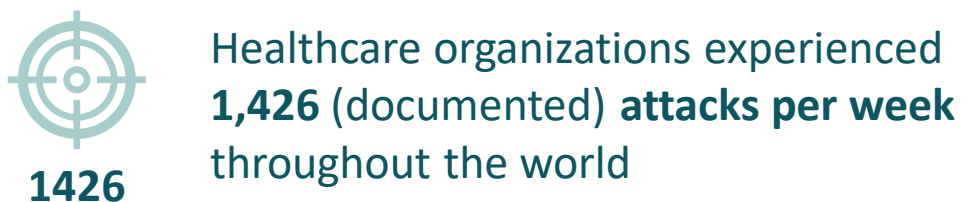
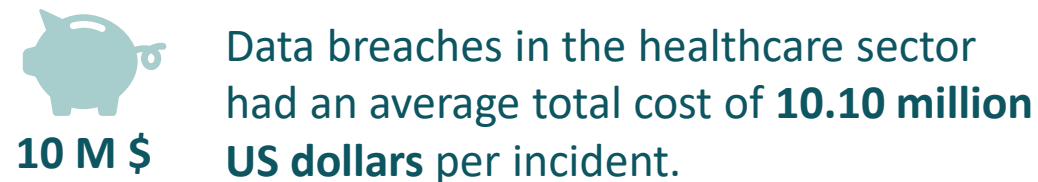
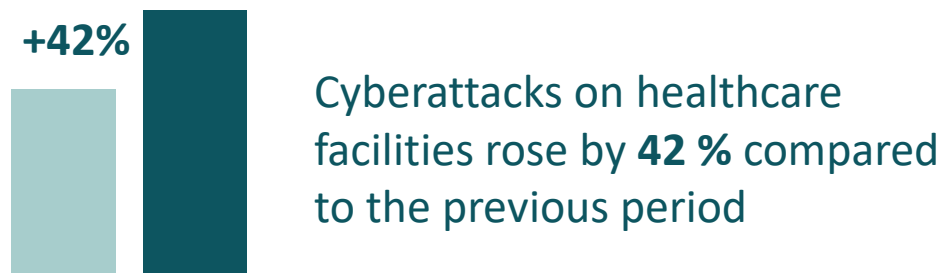
As the recent wave of ransomwares attacks on care facilities (hospitals, retirement homes, etc.) has shown, cyberattacks are increasingly dangerous and threatening in the care sector.

Conclusion: The **danger** of cybercriminality has never been as existential. Our **reliance** on digital tools in all aspects of life makes us **vulnerable** targets, as long as we take no **steps** to ensure our digital safety.

1. Basics of cybersecurity and online safety

1.1. The importance of cybersecurity and online safety

A few numbers from [“Cyber Attack Trends: 2022 Mid-Year Report”](#) show the danger is real. In 2022 alone:



Conclusion: The **danger** of cybercriminality has never been as existential. Our **reliance** on digital tools in all aspects of life makes us **vulnerable** targets, as long as we take no **steps** to ensure our digital safety.

1. Basics of cybersecurity and online safety



1.2. Understanding care workers' responsibility towards patients' data integrity



Trust is the cornerstone, and the foundation of the carer-patient relationship. A central part of this trust is the ability to responsibly handle and safeguard patients' sensitive and personal information.

Patient data encompasses a treasure trove of **personal** and often **sensitive** information.



Medical history



Treatment plan



Life hygiene



Contact details



Social security number

Care professionals are entrusted with large amounts of **personal** and **health** data that can interest a **variety of stakeholders**, from companies selling products, to scammers looking for easy victims or ill-intentioned persons of all kinds.

More importantly and regardless of its value, this data is **personal** and **private**. Care professionals carry the heavy responsibility of keeping them so and owe it to the patients entrusting them with their data.

1. Basics of cybersecurity and online safety



1.2. Understanding care workers' responsibility towards patients' data integrity



While digital treatment of patient data made care workers' lives easier and increased their efficiency, it represents a **vulnerability** and a **new area to protect**.

What about GDPR ? HIPAA?

Legal obligations exist to ensure a minimum of protection and initiate a movement. However, carers should not enact data protection measures only to respect these obligations: it is their **ethical duty** to uphold the **dignity** and **privacy** of patients.

Data protection goes beyond compliance with legal obligations.

Care workers need to realize the **impact** that **data breaches** can have, and to understand the **weight and importance** of their **responsibility**. The trust of their patients depends on this realization, and so does care workers' moral commitment to protecting their patients.

1. Basics of cybersecurity and online safety



1.3. Human errors and negligence are the main entry door for cyber criminality



Human errors and negligence are what cybercriminals exploit. They constitute the easiest **gateway** and equate to leaving the door wide open, without surveillance, after leaving a care facility at night.

Hacking software and databases by exploiting their **technical vulnerabilities** exist, but it is very rare and only accounts for a small part of cyber attacks. In a vast majority of cases, cybercriminals simply walk through the **doors left open** by humans – either through errors or negligence – to gain **unauthorized access** and **compromise sensitive information**.

“I am a care worker, not a geek. Why should I care?”

In almost all the cyberattacks recently witnessed by the care sector (phishing, ransomwares, etc.), the root cause for the breach was not a defective antivirus, a weak software or a suboptimal technical architecture: these attacks almost constantly exploit **human errors**, often from the medical staff itself.

1. Basics of cybersecurity and online safety



1.4. What can we do? Identify and treat human vulnerabilities



Cybersecurity in the care sector is not only about individual efforts – the mistake of one impacts all the others. It is about **collective responsibility, awareness, implementation of best practices and trainings.**

Cybersecurity is an institutionally complex issue, as the mistake of one impacts all (as exemplified with the ransomwares many hospitals fell victims of). Because of this all-encompassing nature, cybersecurity is about **improving the collective defense** against cyber threats, and not just improving individual behaviors.

As such, it implies a **collective effort to raise awareness, increase responsibility and ownership, educate staff** on cyber threats, collectively adopt and apply processes that integrate **best practices**, etc.

At the **individual level**, cybersecurity not only means the **respect of protocols** and processes, but also the understanding of one's position as **actor of the institution's cybersecurity**, implying **critical thinking and awareness raising** about hazards, contribution to **training or mentoring** and **active involvement** and ownership.

1. Basics of cybersecurity and online safety



1.4. What can we do? Identify and treat human vulnerabilities



Cybersecurity is an uncertain science: breaches still happen in well-protected and educated structures.

Corrective measures and preparedness in cases of breaches should not be neglected by organizations.

Even with an improved approach to cybersecurity, better processes, more educated staff, etc. data breaches and cyber attacks might still occur, although significantly less. 100 % protection does not exist, and it is therefore crucial for care institutions to have complete strategies in place that can be rolled out without delay in case of breaches, and to be prepared for crisis management, counteraction, control restoration and impact reduction.

Nonetheless, these strategies are rather to be developed at the level of the **technical teams**, and imply more **specific, technical content**. As such, corrective measures and preparedness are not part of this curriculum, although absolutely necessary for any care organization.

2. Overview of the most common threats

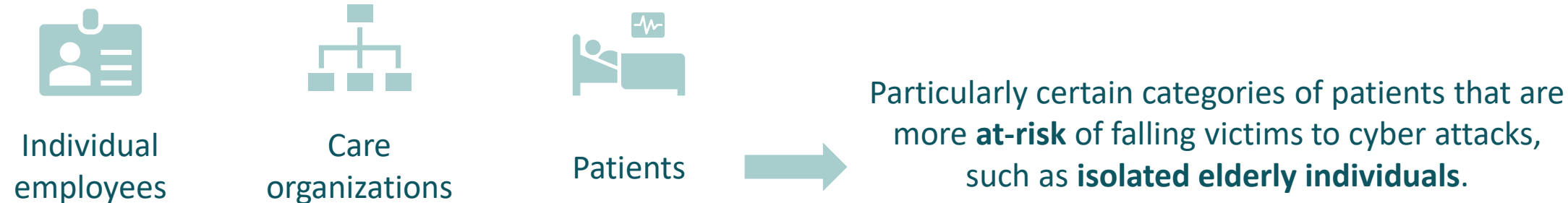
1. Protecting patients
2. Phishing attacks
3. Malwares
4. Social engineering

2. Overview of the most common threats



2.1. Protecting patients

Online threats can target and harm



Care workers can protect their patients when they detect an online risk to their safety by



2. Overview of the most common threats

2.2. Phishing attacks

Phishing attacks are **fraudulent** attempts to **obtain sensitive information** by posing as **trustworthy** entities.

In the care sector, phishing attacks mostly might take the form of:

Business Email Compromise Scams (“Whaling”)

Sophisticated attacks aimed at **tricking** employees into transferring funds or revealing sensitive information.

These scams are often launched by **email** on finance or accounts departments by **impersonating** high-level executives or authorized personnel.

These phishing emails typically request **urgent** payments, changes to vendor details, or sensitive employee information, playing on the **hierarchical relationship** between sender and receiver.

From: CEO@acmecorp.com
To: Jane@acmecorp.com
Subject: Urgent

I need you to initiate a wire transfer in the sum of \$45,250 to the account below. I am boarding a flight and this needs to be done right now. Can you please get this done? Send confirmation of the transfer immediately.

Thanks

Source: [Proofpoint](#)



CLUES

- ✓ Sender uses higher hierarchical position
- ✓ Sense of urgency - no time to check / protest
- ✓ Sender can't talk on the phone, only write
- ✓ Spoofed domain name of the sender's email

2. Overview of the most common threats

2.2. Phishing attacks

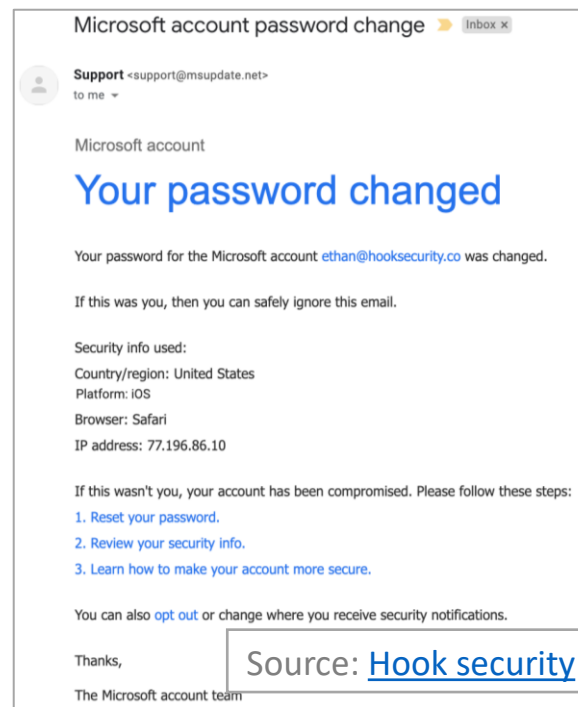
Phishing attacks are **fraudulent** attempts to **obtain sensitive information** by posing as **trustworthy** entities.

In the care sector, phishing attacks mostly might take the form of:

Credential Harvesting Phishing Attacks

Credential harvesting phishing attacks focus on **stealing** usernames, passwords, and other login **credentials** to gain **unauthorized access** to care systems. These scams often use convincing **replicas** of legitimate login pages, such EMR portals or intranets.

Attackers send phishing emails or direct victims to **malicious websites** where they enter their login credentials, **unknowingly** providing cybercriminals the keys to their organization's sensitive data.



CLUES

- ✓ Spoofed domain name of sender's email (ex: @msupdate.net)
- ✓ Different design of the email from the usual emails of the company
- ✓ Request to react to something you have not done (ex: deliver a package you have not ordered).

2. Overview of the most common threats

2.2. Phishing attacks

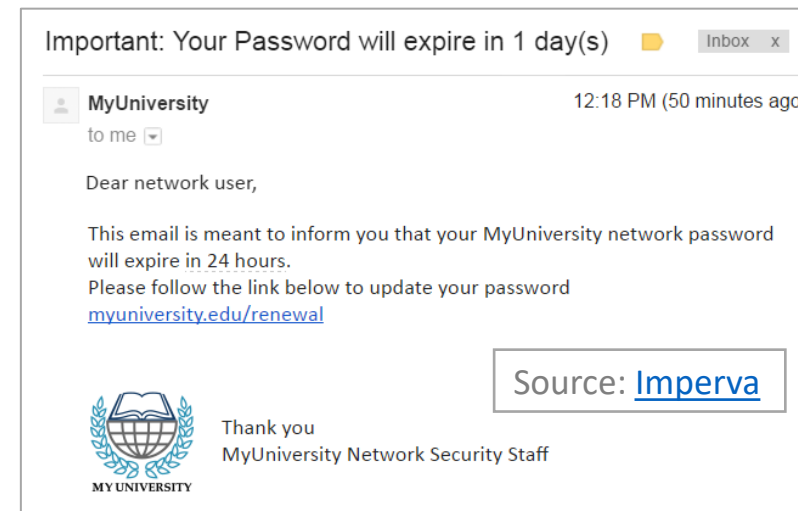
Phishing attacks are **fraudulent** attempts to **obtain sensitive information** by posing as **trustworthy** entities.

In the care sector, phishing attacks mostly might take the form of:

Malware-Laden Phishing Emails

Malware-laden phishing emails are designed to **trick** recipients into downloading and executing **malicious software**. These emails often contain **infected attachments** or **links** to compromised websites.

Healthcare organizations are **particularly vulnerable** to malware attacks, as successful breaches can compromise patient records, disrupt operations, or even endanger lives.



CLUES

- ✓ Spelling, Grammatical and Punctuation Errors
- ✓ Links in the body of the email that redirect to unexpected sites (hover over the link to see the URL)
- ✓ Threat (e.g. blocked account) or sense of urgency
- ✓ Attachments that you did not request / trigger
- ✓ Unusual request, tone or greeting

2. Overview of the most common threats

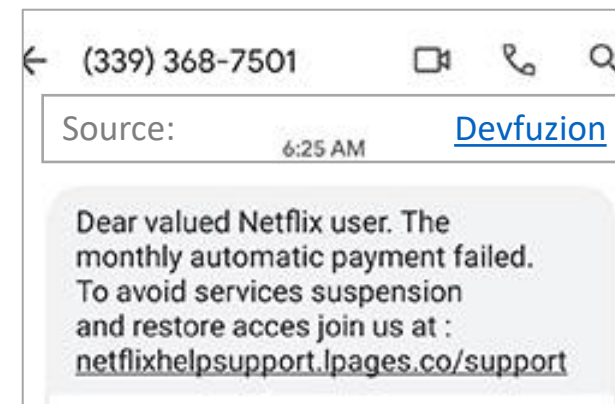
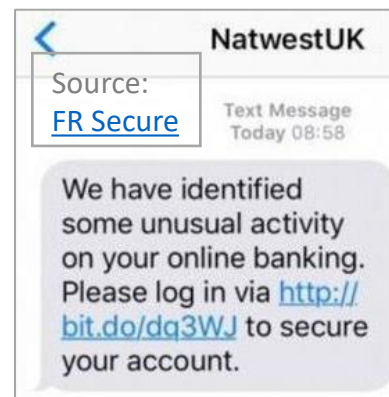
2.2. Phishing attacks


Phishing attacks are **fraudulent** attempts to **obtain sensitive information** by posing as **trustworthy** entities.

In the care sector, phishing attacks mostly might take the form of:

Vishing and smishing attacks

Vishing (by voice messages or phone calls) and **smishing** (by SMS) can be any of the previous phishing attacks. They simply replace the traditional email with another means of communication (SMS, call, etc.).



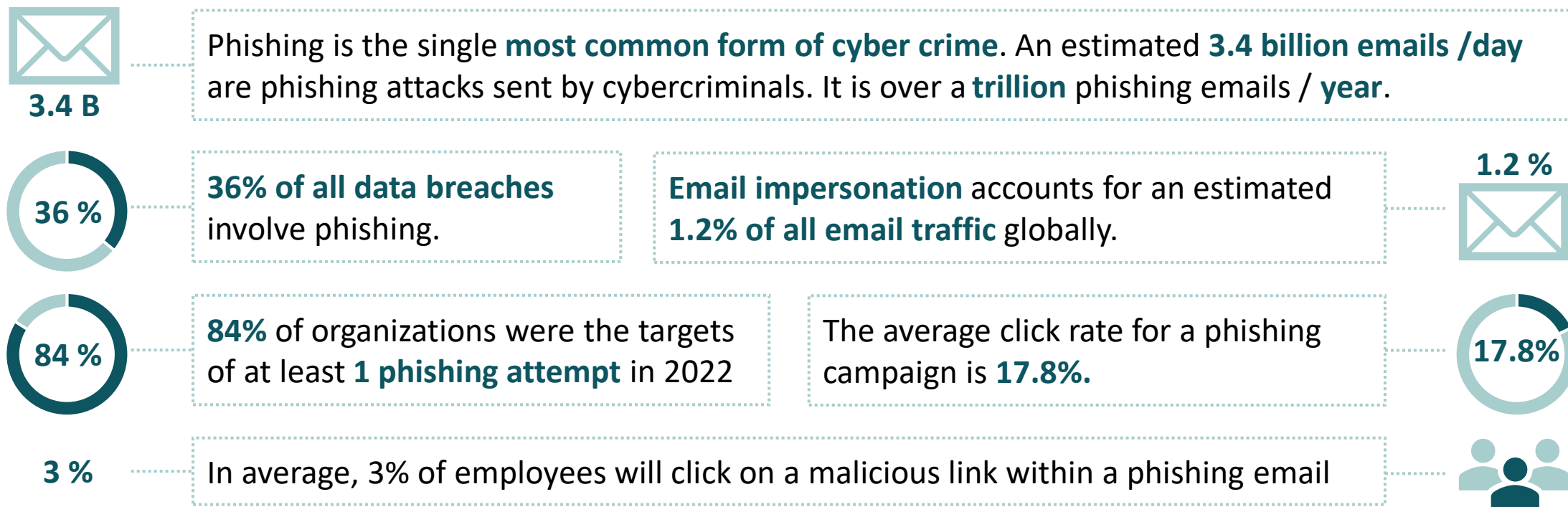
	Vishing	Smishing
 CLUES	<ul style="list-style-type: none">✓ Demanding tone: scammers capitalize on fear or panic✓ Request for confidential or personal information✓ The pretended caller: most of the organizations scammers pretend to represent would not call.	<ul style="list-style-type: none">✓ Unknown number, not referenced on Internet✓ Visit the website of the pretended sender – ex: banks write on their websites that they don't text.✓ Contact the company's customer service directly

2. Overview of the most common threats

2.2. Phishing attacks

Phishing attacks are **fraudulent** attempts to **obtain sensitive information** by posing as **trustworthy** entities.

A few numbers from **2022** show how prevalent, sophisticated and dangerous phishing is (Source: [Stationx.net](https://www.stationx.net))



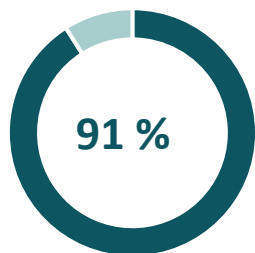
2. Overview of the most common threats



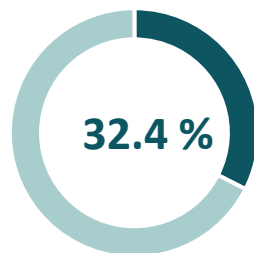
2.2. Phishing attacks

Phishing attacks are **fraudulent** attempts to **obtain sensitive information** by posing as **trustworthy** entities.

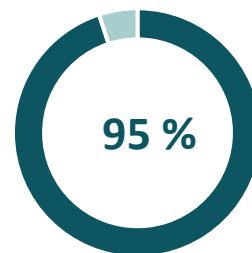
A few numbers from **2022** show how prevalent, sophisticated and dangerous phishing is (Source: [Stationx.net](https://www.stationx.net))



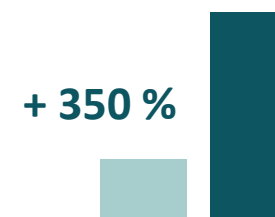
of all cyber attacks begin with a phishing **email**



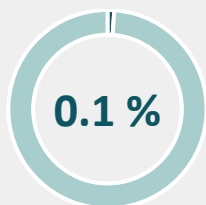
of **untrained** employees can fall for phishing scams



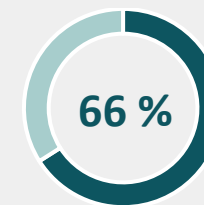
of successful breaches are directly caused by **human error**



Small organizations are **350%** more likely to be **targets** of **phishing** than larger organizations



0.1 % of all email-based phishing attacks are responsible for **66%** of all breaches (*usually targeted, personalized “spear-phishing” attacks*)



2. Overview of the most common threats

2.3. Malwares

Malwares is an umbrella term encompassing various types of malign software designed to disrupt, damage, or gain access to computer systems, networks, or devices. In the care sector, malwares mostly take the form of:

Viruses

Viruses are malicious programs that **infect** other files or software on a computer and replicate themselves when the infected files are **executed**. They can cause damage to data, software, and hardware components.

For example, malware-laden phishing emails or SMS might trick users into clicking on **links** or downloading **files** that are infected. These infected files or links will only be “activated” once the user clicks, hence the need for caution when receiving unsolicited emails.



Many scams use your **fear of viruses** to infect you: if a pop-up message of an antivirus you do not have signals a potential infection of your device and offers to solve it by clicking on a button or calling a number, do not react, it might very well lead you to execute a virus.



Source: [Microsoft community](#)

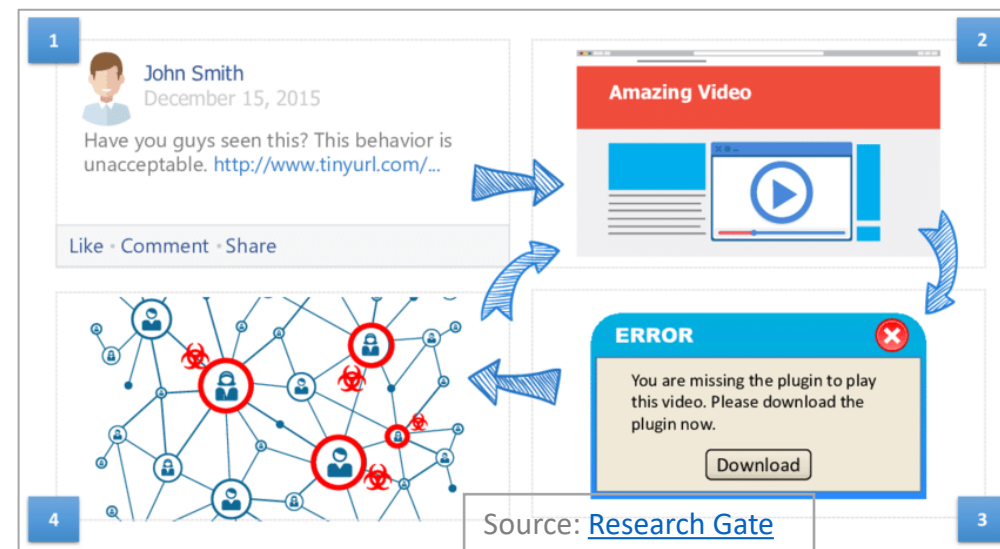
2. Overview of the most common threats

2.3. Malwares

Malwares is an umbrella term encompassing various types of malign software designed to disrupt, damage, or gain access to computer systems, networks, or devices. In the care sector, malwares mostly take the form of:

Trojans

Trojans, or Trojan horses, are malware **disguised as legitimate software**. They trick users into installing them, often by appearing as harmless files or applications. Once installed, Trojans can perform various malicious activities, such as stealing sensitive data, modifying information, or providing unauthorized access to attackers. Trojans are often triggered by phishing emails or messages.



CLUES

- ✓ Computer is running slower than usual.
- ✓ Unauthorized apps are appearing on the device.
- ✓ Frequent crashes and freezes of the device.

- ✓ Frequent pop-ups.
- ✓ Some applications don't start.
- ✓ Frequent interrupted Internet connection.

2. Overview of the most common threats

2.3. Malwares

Malwares is an umbrella term encompassing various types of malign software designed to disrupt, damage, or gain access to computer systems, networks, or devices. In the care sector, malwares mostly take the form of:

Ransomwares

Ransomware is a type of malware that encrypts files on a victim's computer or device, rendering them **inaccessible until a ransom is paid**. Ransomware attacks typically demand payment in cryptocurrency and can cause significant financial and data loss.

Hospitals and health care facilities, whose systems are vital for their operations, are particularly targeted. In 2022, **66%** of hospitals in the US were the **target** (not always victim) of a ransomware attack. Organizations in the healthcare sector **paid** the ransom in about **61%** of ransomware incidents in 2022.



Source: [Healthcare IT News](#)

2. Overview of the most common threats



2.3. Malwares

Malwares is an umbrella term encompassing various types of malign software designed to disrupt, damage, or gain access to computer systems, networks, or devices. In the care sector, malwares mostly take the form of:

Worms

Worms are standalone malware programs that **replicate** themselves across networks, typically exploiting vulnerabilities in operating systems or network protocols.

They can spread rapidly and cause **network congestion** or perform other malicious activities.

Spywares

Spywares are designed to **secretly monitor** and gather information about a user's activities on their computer or device.

They can **track keystrokes, capture screenshots, record browsing habits**, and steal **sensitive information** like passwords and financial data.

Addwares

Addwares are unwanted software that display **advertisements**, often in the form of pop-up ads or browser redirects.

While not inherently malicious, adware can **degrade system performance**, compromise user **privacy**, and lead to **further infections** if not removed.

2. Overview of the most common threats

2.3. Malwares

Malwares is an umbrella term encompassing various types of malign software designed to disrupt, damage, or gain access to computer systems, networks, or devices. In the care sector, malwares mostly take the form of:

Keyloggers

Keyloggers are a type of spyware that record **keystrokes** typed by a user, capturing sensitive information such as **passwords**, **usernames**, and **credit card** details.

Attackers can use keyloggers to steal personal information and commit identity theft.

Botnets

Botnets are **networks of compromised computers** or devices controlled by attackers.

Botnets can be used to carry out distributed **denial-of-service (DDoS)** attacks, send **spam emails**, or perform other malicious activities **without the owners' knowledge**.

Backdoors

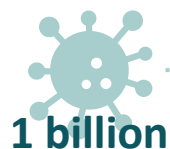
Backdoors are **hidden entry points** or vulnerabilities intentionally created by attackers in software or systems, allowing **unauthorized access for future exploitation or control**.

These backdoors allow attackers to **secretly and remotely** take control of the device, install other malwares, record keystrokes, etc.

2. Overview of the most common threats

2.3. Malwares

These different types of malwares are often combined within one program or file. A few numbers from **2022** show how prevalent, sophisticated and dangerous malwares are (Source: [Getastra.com](https://getastra.com))



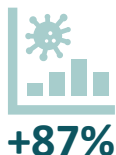
560 000 new pieces of malware are detected **daily**. Over **1 billion malware** programs exist currently.



Every minute, 4 companies fall victim to ransomware attacks. The **care sector** is the most targeted, and the one that pays ransoms most. The average cost of a ransomware attack is **\$4.54 million**.



In ransomware incidents, only **50%** of the organizations that paid the **ransom** managed to **retrieve their data**. **64%** of organizations targeted by ransomware attacks were actually **infected**.



Over the past decade, there has been **an 87% increase** in malware infections. **Trojans** account for **58%** of all computer malware. The cost of cybercrime is predicted to reach **\$8 trillion in 2023**.

2. Overview of the most common threats

2.4. Social engineering

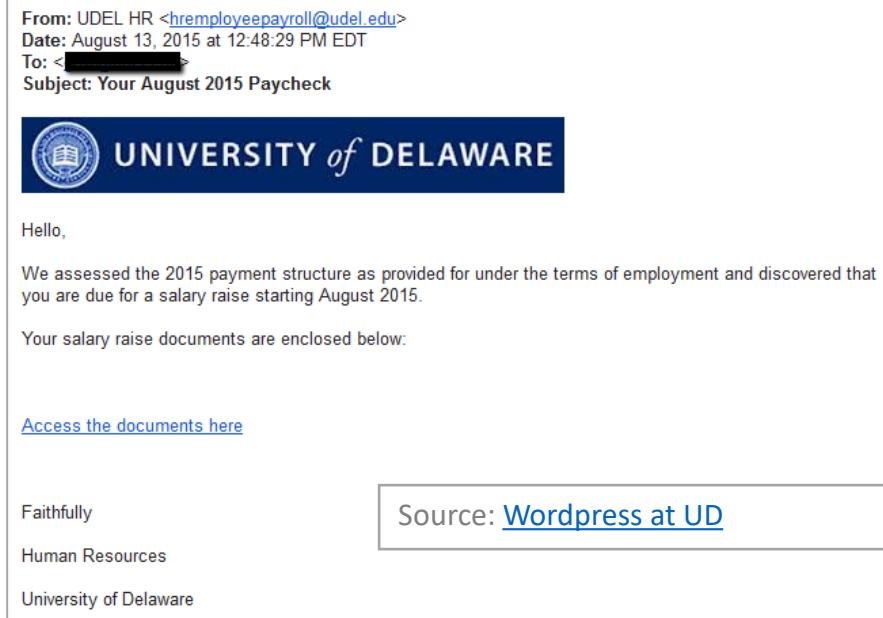
Social engineering refers to the use of social tactics to exploit employees' trust, negligence or unawareness to obtain confidential information. While phishing and malware attacks often exploit these vulnerabilities and **overlap** with social engineering, pure social engineering more directly uses **social tactics**, and might include:

Spear phishing

Spear phishing is a **targeted form of phishing** that **tailors the attack** to specific individuals or organizations.

Attackers gather information about their targets from social media, public databases, or previous interactions to personalize the phishing emails and increase the likelihood of success.

Spear phishing messages can entail malwares of different types, directly request personal data (e.g. phone number to solve an “urgent matter”), ask for an invoice payment, etc.



2. Overview of the most common threats



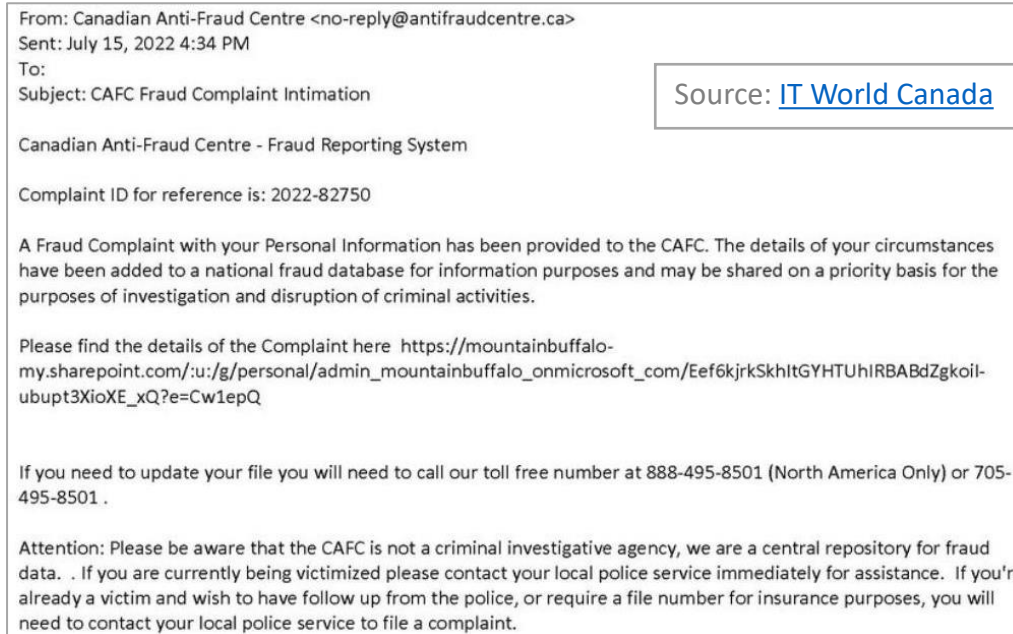
2.4. Social engineering

Social engineering refers to the use of social tactics to exploit employees' trust, negligence or unawareness to obtain confidential information. While phishing and malware attacks often exploit these vulnerabilities and **overlap** with social engineering, pure social engineering more directly uses **social tactics**, and might include:

Pretexting

Pretexting involves creating a **fabricated scenario or pretext** to manipulate individuals into disclosing confidential information or performing specific actions.

Attackers often impersonate **trusted entities**, such as IT support personnel, law enforcement officers, or company executives, to gain the target's trust and obtain sensitive information. Pretexting scams can have very similar outcomes to any type of phishing scam, requesting payment, stealing credentials or personal data, etc.



2. Overview of the most common threats

2.4. Social engineering

Social engineering refers to the use of social tactics to exploit employees' trust, negligence or unawareness to obtain confidential information. While phishing and malware attacks often exploit these vulnerabilities and **overlap** with social engineering, pure social engineering more directly uses **social tactics**, and might include:

Baiting

Baiting relies on the **curiosity or greed** of individuals to lure them into downloading malicious files or visiting compromised websites. Attackers offer **enticing bait**, such as free software downloads, movie downloads, or gift cards, which contain malware or lead to phishing pages when accessed.

Baiting is often linked to some kind of pretexting, spear phishing, impersonation, etc. to target the user's **vulnerabilities** and enhance the sender's **credibility**.



Source: [Dummies.com](https://www.dummies.com)

2. Overview of the most common threats



2.4. Social engineering

Social engineering refers to the use of social tactics to exploit employees' trust, negligence or unawareness to obtain confidential information. While phishing and malware attacks often exploit these vulnerabilities and **overlap** with social engineering, pure social engineering more directly uses **social tactics**, and might include:

Tailgating (Piggybacking):

Tailgating, or piggybacking, involves **physically gaining unauthorized access** to restricted areas or systems by following behind an authorized individual.

Attackers exploit **human courtesy or lack of awareness** to enter secure premises without proper authorization.

Watering hole attacks

Watering hole attacks target specific groups or organizations by **infecting websites frequented by their members** with malware.

Attackers compromise legitimate websites to **distribute malware** to unsuspecting visitors, exploiting their trust in the compromised site.

Impersonation (Identity Theft):

Most phishing tactics imply some form of impersonation. But some include additional elements to enhance credibility, that constitute **identity theft**.

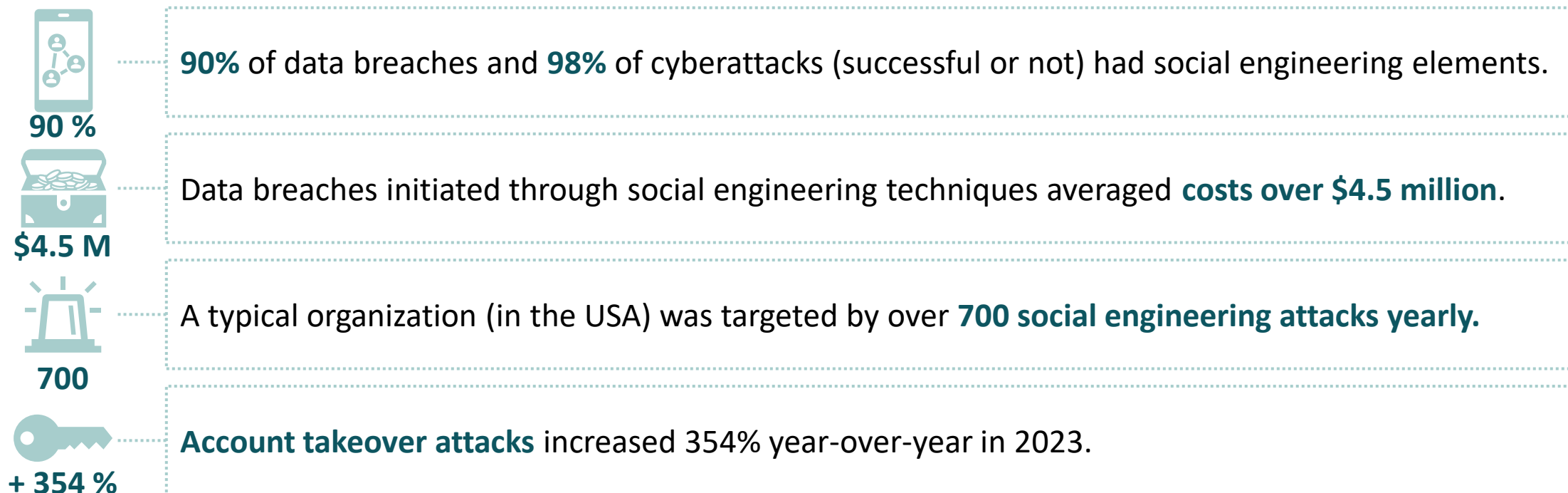
These may include stolen or forged credentials and documents, IA-created elements, etc. to **deceive** about their authenticity.

2. Overview of the most common threats



2.4. Social engineering

Social engineering often represents a gateway to deliver malware or induce victims to perform an action. A few numbers from **2023** show how prevalent, sophisticated and dangerous social engineering is (Source: [Resmo](#))



3. Preventive measures

1. Password security
2. Two-factor authentication (2FA)
3. Anti-virus
4. Software updates
5. Network security
6. Data backup

3. Preventive measures

3.1. Password security

Why is it important ?

Password security is the **first weakness** exploited by cybercriminals. **Stronger** passwords (i.e. more complicated and diverse) are harder to guess or uncover using brute-force attacks and can therefore be an adopt, useful **first line of defence** against cyberattacks.



What can I do ?

- Set **strong** passwords: at least **16** characters, with uppercase and lower-case letters, numbers and special characters.
- **Transform sentences** into passwords rather than words, using a code to transform various types of letters. Ex: “Icàre@b0utSecur1ty!”
- Use **password managers** remembering your passwords for you and generating passwords.



What can my organization do ?

- Configure your systems (email, online messaging tools, ERP, CRM, etc.) to force users to **renew their password regularly**. This will shorten the amount of time a given password remains valid.
- Configure **password rules** to ensure that users don't use the **same password twice** and that the password is **strong enough**.
- Force a general **password renewal** after a breach.

3. Preventive measures

3.1. Password security

Why is it important ?

Password security is the **first weakness** exploited by cybercriminals. **Stronger** passwords (i.e. more complicated and diverse) are harder to guess or uncover using brute-force attacks and can therefore be an adopt, useful **first line of defence** against cyberattacks.



ZOOM on password managers

- Password managers **store your passwords** and relieve you from the duty of remembering them. As cloud solutions, they remain **accessible from other devices**.
- Password registration can be made **manually** or **automatically**. You can also set the password manager to auto-fill the password field when connecting to your accounts.
- Better, password managers can **generate unique, very strong passwords** for each of your accounts and remember them for you. You won't even have to know them.
- All you have to remember is **one very strong password** – the one giving you access to the password manager.



Useful tools

- [Dashlane](#)
- [1Password](#)
- [LastPass](#)
- [Bitwarden](#)

3. Preventive measures

3.2. Two-factor authentication (2FA)

Why is it important ?

2FA drastically improves security: this authentication method requires the use of at least **two devices** to log into an account, both of which need to be **registered** and **trusted** beforehand. This method not only gives the user **control** over an account that might have been compromised but can also **indicate** that it has been.



What can I do ?

- **Enable 2FA** as early as possible – it will be too late once a password or account is compromised.
- In most software and websites, you will find the ability to enable it under **Settings > Security** (IOS and Microsoft, Google services, social media, etc.)
- The most used and reliable method is the use of **two devices** belonging to the user (e.g. phone and computer) registered on an account.



What can my organization do ?

- For most systems, your IT department can enforce **2FA system-wide** for all users. 2FA might also be referred to as “two-step verification” or “multi-factor authentication”.
- However, this requires all **employees to have access to 2 devices**, ideally for professional-use only, which might not be the case. Alternatively, employees can be **encouraged** to enable 2FA.

3. Preventive measures

3.2. Two-factor authentication (2FA)

Why is it important ?

2FA drastically improves security: this authentication method requires the use of at least **two devices** to log into an account, both of which need to be **registered** and **trusted** beforehand. This method not only gives the user **control** over an account that might have been compromised but can also **indicate** that it has been.



How do I do it?

- [Google Workspace](#) (Gmail, Gdrive, Calendar, etc.)
- [Microsoft 365](#) (Outlook, OneDrive, Teams, etc.)
- [Slack](#)
- [Zoom](#)

And others – generally available in the **security session of the Settings** for most digital tools – including for personal use (social media, banking, e-commerce, governmental applications and websites, etc.).

3. Preventive measures



3.3. Anti-virus

Why is it important ?

Anti-virus protect their owner by **scanning potential threats and detecting risks**, from email phishing or malware attempts to fraudulent websites and programs. This protection also extends beyond the computer to any **external devices** interacting with it, such as USB sticks that might be carrying malwares too.



What can I do ?

- **Autonomously install** an anti-virus software if not provided by your organization (or **advocate** for it to be done organization-wide). Unprotected computers are **easy targets** to cybercriminals.
- Remember that anti-viruses are additional layers of a **security that still depends on the human factor**: keep the **same level of vigilance** online, whether you are “protected” or not.



What can my organization do ?

Your IT department can and **should** install, configure and manage updates of a **system-wide anti-virus software**, to ensure that the organization’s digital security is better protected.



Useful tools

[ESET](#)
[Kaspersky](#)

[Bitdefender](#)
[AVG](#)

3. Preventive measures



3.4. Software updates

Why is it important ?

Keeping software and operating systems **up to date** prevents cybercriminals from exploiting known **security issues**: software providers regularly stress-test their own security. When they discover potential safety breaches, they **release updates** removing these vulnerabilities or making them unexploitable.



What can I do ?

Do not delay the update of all software and applications you use (personally and professionally) when you receive an update notification. Regularly verify that all is up-to-date in your application center.



What can my organization do ?

Your IT department can configure automatic updates for operating systems and applications used in the entire organization, select when and how often to install them without disrupting operations.



How do I do it?



[On Windows](#)

[On Mac](#)



[On Android](#)

[On IOS](#)



Useful tools

[Manage updates on Windows](#)

[Turn on automatic app updates](#)

[Update MacOS](#)

[on Mac](#)

3. Preventive measures



3.5. Network security - VPN

Why is it important ?

When it is necessary for workers to access information from **outside of the premises**, it becomes harder for IT staff to have **control over all security aspects**. **Virtual Private Networks (VPN)** enable the creation of a **direct, secure and isolated network** between two machines and allows them to interact and exchange data.



How does it work?

A VPN is a technology that creates a **secure and encrypted** connection over the internet. VPNs encrypt data transmitted between the user's device and the VPN server, preventing third parties from intercepting and accessing the data. This encryption is an **additional layer of security**, ensuring that sensitive information, such as passwords, credit card details, and personal communications, remain secure.

In the context of care workers, VPNs will mostly **secure remote access** to private networks and resources, such as corporate intranets, servers, or databases, notably for those working on the field. They will also provide **increased security** for those connecting to Internet via **public**, and generally unsecured **Wifi networks**.

3. Preventive measures



3.5. Network security - VPN

Why is it important ?

When it is necessary for workers to access information from **outside of the premises**, it becomes harder for IT staff to have **control over all security aspects**. **Virtual Private Networks (VPN)** enable the creation of a **direct, secure and isolated network** between two machines and allows them to interact and exchange data.



What can my organization do ?

VPNs should be installed, when there is a need, by the **organizations' technical department**, as it will mostly be used as a **system-wide geographical extension of the existing network**, preventing the individual user from installing it autonomously. Individuals can, however, **advocate** for a VPN to their IT department or management.

VPNs may require the **installation of a software** on the machines that need to be interconnected as well as an **authentication method** prior to accessing the network. They can be configured to only work on certain devices, in certain locations and at certain times to restrain external access, while still giving the workers who need it access to the necessary data.

3. Preventive measures

3.6. Data backup

Why is it important ?

One of the main threats of cyber attacks is **the altering of sensitive data**, specifically patient data. Ensuring its security and integrity is of absolute importance, even in the face of a cyberthreat. A robust **institutional data backup strategy**, with regular **backup procedures** and **high staff compliance** is the key to securing data integrity.



What can I do ?

- As individual workers, the first measure to ensure data integrity and security is the **compliance to the different protocols** set by the technical department, to **undergo regular training** and to **consider the matter seriously** and consistently.
- As actor of your own organization's security, you can also **enquire** about your data backup strategy, **propose** and **advocate** for modifications.



What can my organization do ?

Designing and implementing an **institutional data backup strategy** is the responsibility of the technical department. Such a strategy should include **measures ensuring staff compliance**, procedures for **regular data backup** on a **cloud-storage solutions** (Gdrive, Onedrive, etc.) or a network-attached storage, providing a safety net for the **swift recovery of data** in case of a breach questioning data integrity.

4. Best practices and good habits

1. Physical space
2. Secure browsing
3. Secure emailing
4. Safe social media use
5. Mobile device security
6. Password security

4. Best practices and good habits



4.1. Physical space

Cybersecurity starts offline: before setting technical defenses, make sure to organize your physical space in a secure way, that will reduce hazards and vulnerabilities.

1. Lock your devices when not in use
2. Secure your workspace from unauthorized access
3. Adopt a clean desk policy
4. Use privacy screens
5. Shred sensitive documents
6. Do not write down passwords
7. Be mindful of shoulder surfing
8. Enable full-disk encryption

4. Best practices and good habits

4.1. Physical space

Cybersecurity starts offline: before setting technical defenses, make sure to organize your physical space in a secure way, that will reduce hazards and vulnerabilities.

1. Lock your devices when not in use

Always **lock** your computer, laptop, tablet, or phone when they are not in use, especially in public or shared spaces. Use strong passwords, PINs, or biometric authentication (e.g., fingerprint or facial recognition) to secure your devices and prevent unauthorized access.



Tips

- On Windows, use the shortcut Windows + L to lock your screen.
- On Mac, use the shortcut Control-Command-Q to lock your screen.

2. Secure your workspace from unauthorized access

- Keep your workspace **free from unauthorized individuals**. Ensure that physical access points, such as doors, windows, or entryways, are secured and monitored to prevent unauthorized entry to your workspace or premises.
- **Lock** drawers, cabinets, or file cabinets containing sensitive documents, devices, or storage media when not in use.
- Secure **peripherals** such as keyboards, mice, and external storage devices (USB, hard drive, etc.) and store them in locked drawers or cabinets.

4. Best practices and good habits

4.1. Physical space

Cybersecurity starts offline: before setting technical defenses, make sure to organize your physical space in a secure way, that will reduce hazards and vulnerabilities.

3. Adopt a clean desk policy

Adhere to a **clean desk policy** by removing sensitive documents, notes, or passwords from your desk when you're not present. Store physical documents securely, preferably in locked cabinets or drawers.



Tips

A good practice is to aim for a “0-paper desk”, with only the papers currently being used on the desk. Not only is it proven to increase efficiency and reduce stress, it also decreases the risk of leaving important information visible by unauthorized people.

4. Use privacy screens

Use **privacy screens or filters** on computer or mobile devices to prevent unauthorized viewing of your screen. Privacy screens force viewers to be exactly in front of the device and prevent shoulder-surfing. They are built-in on certain devices or can be downloaded.



Tips

- On computers with built-in privacy screens, press F12 or Fn + D to activate it.
- On Android, best-rated privacy screen apps are 1) Privacy Screen, 2) Screen Guard privacy, 3) Privacy filter

4. Best practices and good habits



4.1. Physical space

Cybersecurity starts offline: before setting technical defenses, make sure to organize your physical space in a secure way, that will reduce hazards and vulnerabilities.

5. Shred sensitive documents

Shred or securely dispose of physical documents containing sensitive information, such as financial records, personal identification, etc. before discarding them. Do not simply throw in the bin without **at least tearing** a document.



Tips

While recycling is any worker's responsibility today, remember that loose paper is often left unattended before it is recycled, and it can leave your organization vulnerable to potential security breaches if sensitive.

6. Do not write down passwords

Do not write down passwords or PINs on sticky notes, notebooks, or physical documents. If writing a password is absolutely necessary, do so in a place where it can not be found and encrypt it with a code only you can decipher (ex: # of children of sister / dog's birthday month, etc.)



Tips

Instead, use a reputable password manager to securely store and manage passwords. The only password you will need to remember is that of the password manager.

4. Best practices and good habits

4.1. Physical space

Cybersecurity starts offline: before setting technical defenses, make sure to organize your physical space in a secure way, that will reduce hazards and vulnerabilities.

7. Be mindful of shoulder surfing

Be aware of your surroundings and protect your screen and keyboard from being viewed by unauthorized individuals, specifically in public spaces. **Shield your keypad** when entering PINs or passwords on ATMs, keypads, or mobile devices.



Tips

- Privacy screens are a good way to fight against shoulder surfing.
- When in a public space, privilege sitting with your back against a wall to prevent shoulder surfing from behind.

8. Enable full-disk encryption

Enable **full-disk encryption** on your devices to protect data stored on the device's hard drive or storage media. This ensures that even if your device is stolen or lost, unauthorized users cannot access the data without the encryption key.



Tips

- On Windows, enable encryption in Settings > Privacy and Security
- Most mobile operating systems now also possess features allowing to remotely delete data in case of loss of the device.

4. Best practices and good habits



4.2. Secure browsing

When **browsing** on Internet, make sure to uphold the following best practices.

1. Use secure websites (HTTPS)
2. Keep your software and operating system up to date
3. Use ad-Blockers and content filters
4. Be cautious with downloads
5. Browse anonymously
6. Regularly clear browser cache and cookies

4. Best practices and good habits

4.2. Secure browsing

When **browsing** on Internet, make sure to uphold the following best practices.

1. Use secure websites (HTTPS)

Look for **HTTPS** in the website URL to ensure a secure connection when transmitting sensitive information, such as login credentials or financial details. Avoid entering personal information on websites that only use **HTTP**.



Tips

HTTP messages are plaintext, which means unauthorized parties can easily access and read them over the internet. HTTPS transmits all data in encrypted form. When users submit sensitive data, no third parties can intercept the data over the network.

2. Keep your software and OS up to date

Regularly update your operating system (OS), web browser, antivirus software, and other applications to patch known vulnerabilities and protect against security threats.



Tips

Do not delay the update of all software and applications you use (personally and professionally) when you receive an update notification. Regularly verify that all is up-to-date in your application center.

4. Best practices and good habits

4.2. Secure browsing

When **browsing** on Internet, make sure to uphold the following best practices.

3. Use ad-Blockers and content filters

Install **ad-blockers and content filters** to prevent malicious advertisements, pop-ups, or scripts from compromising your browsing experience or delivering malware. Certain websites might require you to deactivate it to access content, which can easily be done from the icon on your browser.



Best-rated free Adblockers:

- uBlock origin
- Privacy Badger
- Ghostery
- Adblock plus

Tips

4. Be cautious with downloads

Download software, files, and attachments only from **reputable sources** and avoid downloading content from untrusted websites or unknown sources to minimize the risk of malware infections.



An incredible amount of content is available on Internet. If a website requires you to download something, you can probably access similar content from another website, without downloading anything.

Tips

4. Best practices and good habits



4.2. Secure browsing

When **browsing** on Internet, make sure to uphold the following best practices.

5. Browse anonymously

Consider using a **virtual private network (VPN)** to **encrypt** your internet traffic and browse anonymously, especially when using public Wi-Fi networks or accessing sensitive information.



Tips

Do not mistake the “incognito” mode or “private browsing” mode for a VPN: they do not make your browsing any safer: they simply erase your browsing history from your device. But your browsing history is still visible to the outside world, as well as your IP address, network, etc.

6. Regularly clear browser cache and cookies

Periodically **clear** your browser cache, cookies, and browsing history to remove **tracking data** and minimize the risk of unauthorized access to your browsing habits or personal information.



Tips

On Chrome, click on the 3 dots in the top-right corner > Delete browsing data. In the new opened tab, select the period you want to clear data for (ideally “All time”), select the three options (browsing history, cookies and cache) and click “Delete browsing data” to clear your browser at once.

4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

1. Do I know and recognize the sender?
2. Is the email unexpected or unsolicited?
3. Does the email address me by name?
4. Are there spelling or grammar errors?
5. Are there suspicious attachments?
6. Does the email contain unexpected links?
7. Is the email asking for sensitive information?
8. Do the signature and contact info look legit?
9. Do I have an existing relationship with the sender?
10. Is the email using threats or fear tactics?
11. Did the anti-virus detect anything suspicious?
12. Does it look like other emails from that provider?

In addition, make sure to always treat an email with the following **attitude**:

- Do **never take immediate, precipitated action**
- **Always assume** that an email might be a **scam**, take your time to study and “clear” it
- **Trust your judgement** and instincts: if something feels off, explore it with caution.
- Remember that scams play on **emotions** like fear, through intimidation and threats. Keep a **cold head** and stay **calm** in all cases.

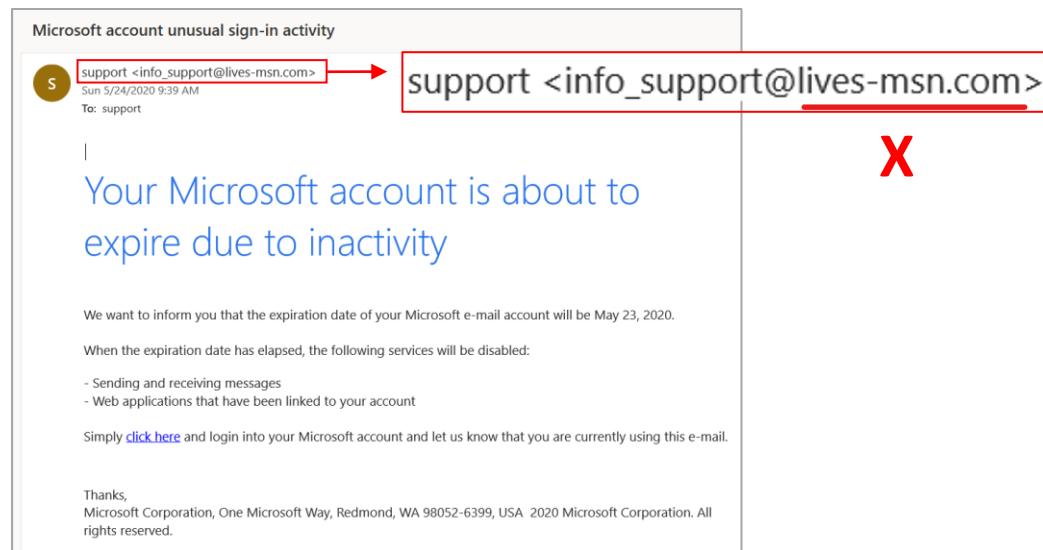
4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

1. Do I know and recognize the sender?

Verify the identity of the sender, not only by viewing the name displayed on top and in the signature, but also the **actual email address** that sent the email.



2. Is the email unexpected or unsolicited?

Be wary of unexpected emails, especially those claiming **urgent action** or offering **unsolicited services**.

Scammers often use them to trick recipients, most commonly using these topics:

- Need to update or verify account information (account suspension, expiration, security alert, etc.)
- Need to pay a pending invoice through a link
- Offers of fake job opportunities
- Payment or remote access to computer or account requested by “support” to solve technical issues.
- Need to pay processing fees or provide personal information to obtain an unsolicited reward or prize.

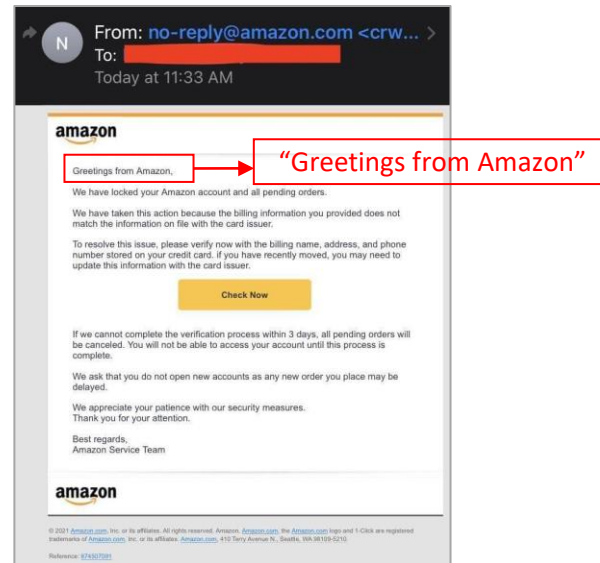
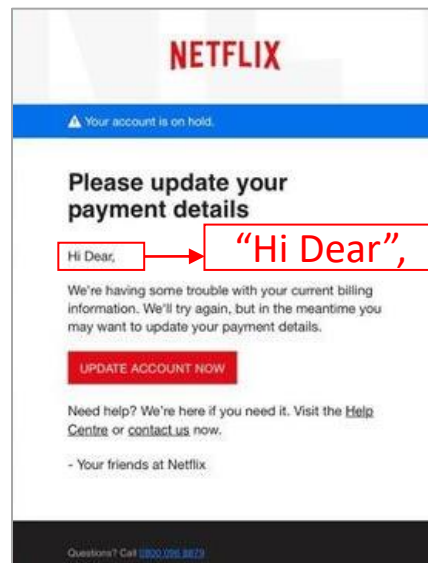
4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

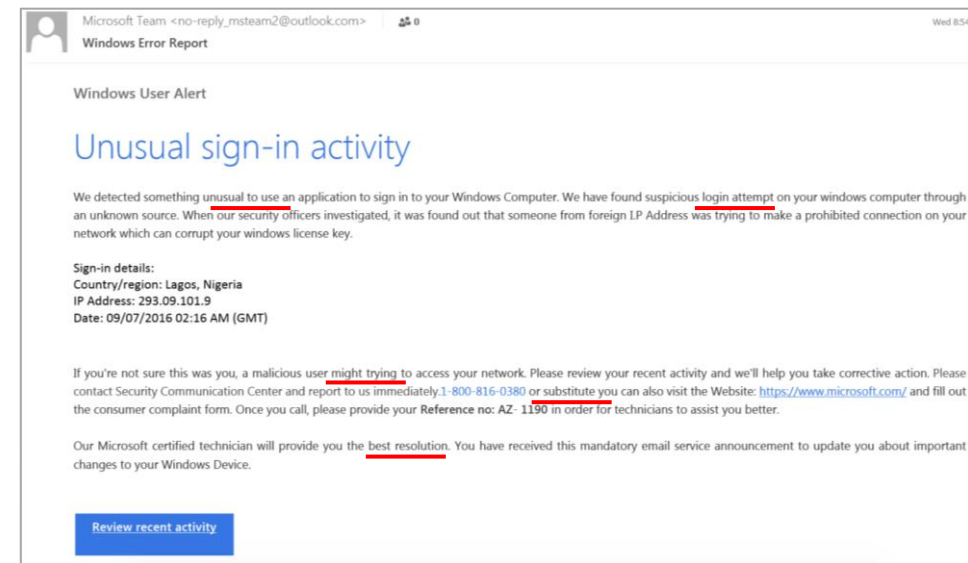
3. Does the email address me by name?

Legitimate organizations often use your name in their communications. **Generic greetings** or **misspellings** of your name can be red flags.



4. Are there spelling or grammar errors?

Poorly written emails, with **spelling** or **grammar mistakes** can indicate a phishing attempt. Legitimate organizations generally do less mistakes in their emails.



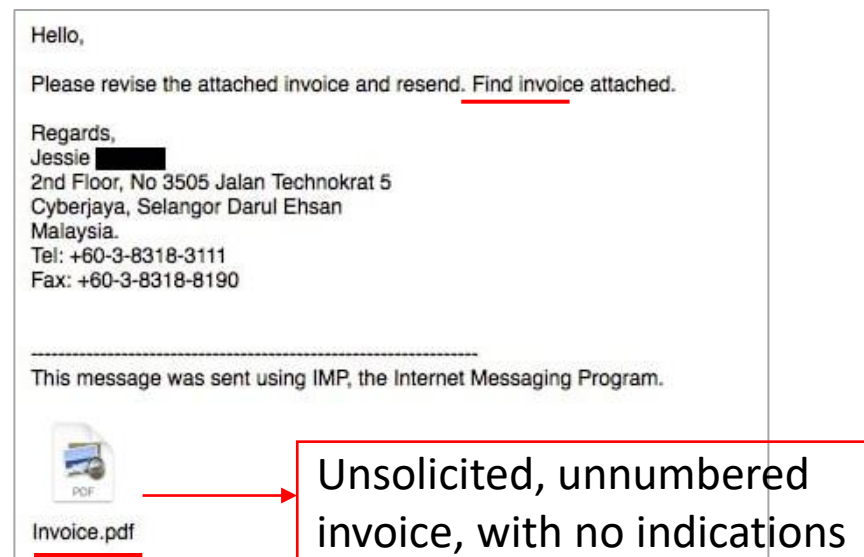
4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

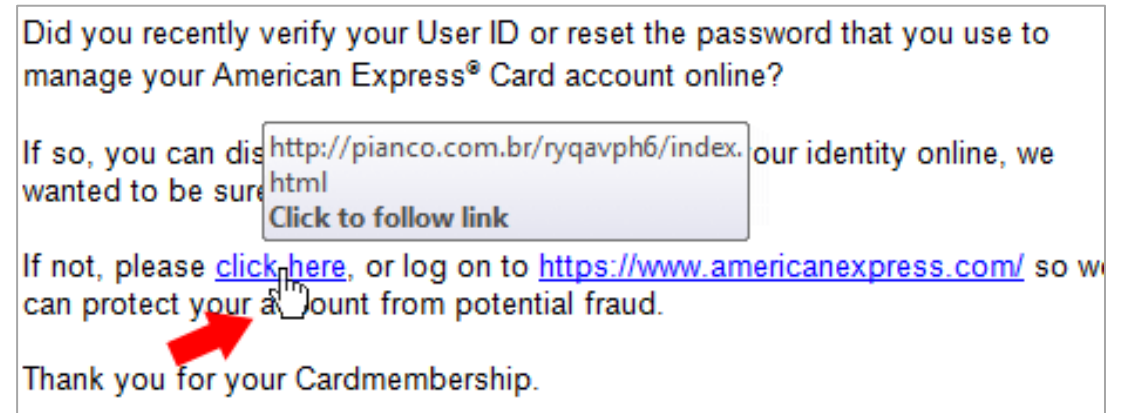
5. Are there suspicious attachments?

Avoid opening **unexpected attachments**, especially from unknown sources. Malicious attachments can contain **malware** or **phishing** attempts.



6. Does the email contain unexpected links?

Hover over any links in the email without clicking to see the **actual URL**. If the link doesn't match the purported sender's official website or looks suspicious, it could be a phishing attempt.



4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

7. Is the email asking for sensitive information?

Organizations normally **don't request sensitive information** by email or via link (such as passwords or credit card details) but normally prompt you to connect to **your account** on their website.



We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

8. Do the signature and contact info look legit?

Legitimate organizations usually provide **clear contact information** in their emails, including a **physical address**. Verify the sender's details, including their **signature**, and cross-reference them with official sources.

Microsoft account unusual sign-in activity

Microsoft account team <account-security-noreply@accountprotection.microsoft.c>
10:36 AM

To: aivering@live.com

Microsoft account

Verify your account

We detected something unusual about a recent sign-in for the Microsoft account a*****@live.com. For example, you might be signing in from a new location, device, or app.

To help keep you safe, we've blocked access to your inbox, contacts list, and calendar for that sign-in. Please review your recent activity and we'll help you secure your account. To regain access, you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft account team

Déclaration de confidentialité

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

✓ Actual MS contact details

X - No contact details

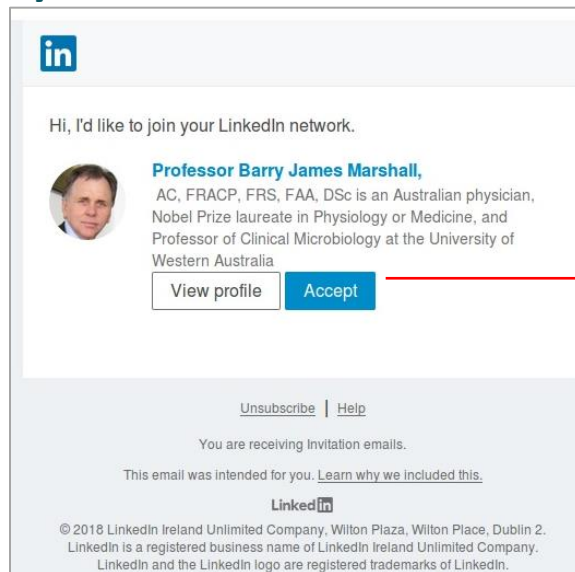
4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

9. Do I have an existing relationship with the sender?

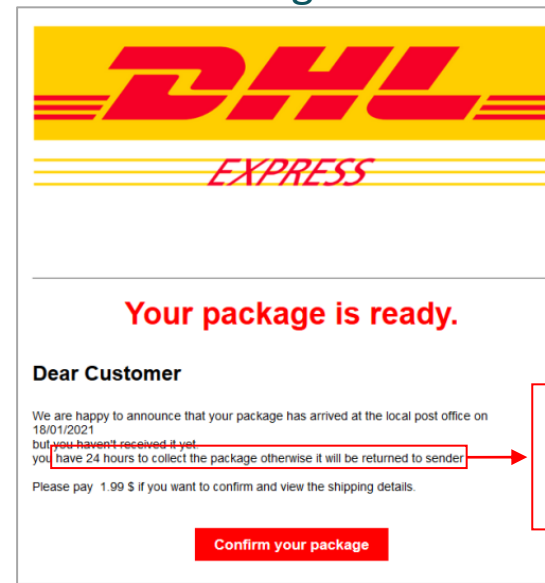
If the email claims to be from an organization you have an account with, verify the information **from your account** rather than relying solely on an email.



Check on LinkedIn account rather than clicking "Accept"

10. Is the email using threats or fear tactics?

Scammers use **threats, intimidation, or fear** tactics to pressure recipients into taking rapid action. Be wary of emails creating a sense of **urgency or fear**.



"You have 24 hours to collect the package otherwise it will be returned to sender"

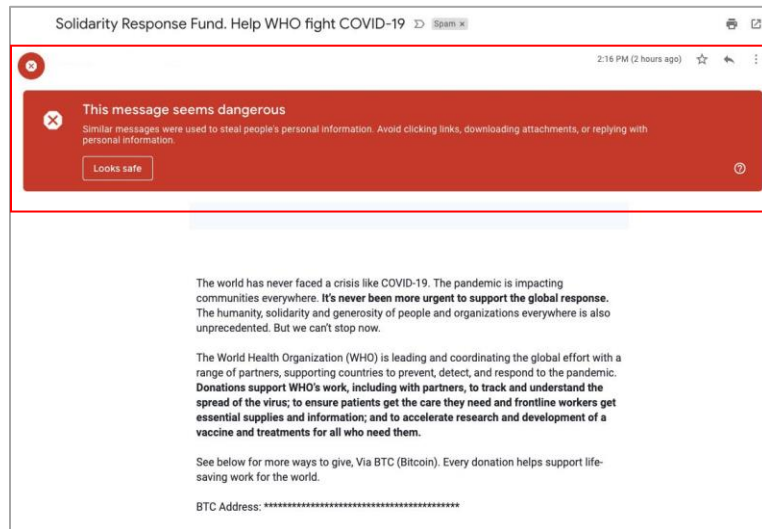
4. Best practices and good habits

4.3. Secure emailing

When receiving an email, make sure to ask yourself the following questions to prevent any security issue:

11. Did the anti-virus detect anything suspicious?

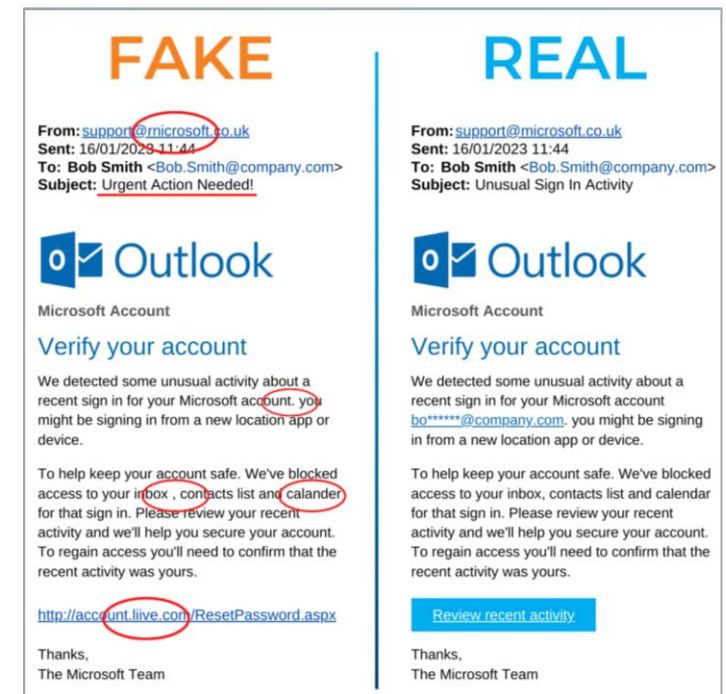
Most email providers have **built-in modules** detecting phishing attempts. Besides, your own **anti-virus** might have flagged the email as **suspicious**. If so, proceed with **caution** with the email.



“This message seems dangerous”

12. Does it look like other emails from that provider?

When receiving an email presumably from an organization you **already have received emails** from, verify that the design, branding, contact details, copyright, links, and language **match** before trusting it.



4. Best practices and good habits



4.4. Safe social media use

Safely use social media by integrating the following practices.

1. Review and adjust privacy settings
2. Be selective with friend requests and connections
3. Beware of phishing and scams
4. Be mindful of location sharing and of what you post
5. Verify account authenticity
6. Monitor third-party apps and permissions

4. Best practices and good habits



4.4. Social media and messaging

Safely use social media by integrating the following practices.

1. Review and adjust privacy settings

Regularly **review and adjust your privacy settings** on social media platforms to control who can see your posts, personal information, and photos.

Limit the audience for your posts and consider **restricting access** to sensitive information to trusted friends and contacts.



Tips

Most default privacy settings on social media may permit the sharing of your information with other third-party online users, including your name, age, place of residence, gender, etc.

2. Be selective with friend requests and connections

Be cautious when accepting **friend requests or connections** from unknown individuals. Verify the identity of the person before accepting their request, especially if you don't know them personally. Many social media scams start by becoming “your friend” and **accessing more of your data**.



Tips

Try to verify the authenticity of the request through other means. Ex: if you receive a request from someone claiming to be your friend's brother, you can ask your friend to confirm the person's identity before accepting.

4. Best practices and good habits

4.4. Social media and messaging

Safely use social media by integrating the following practices.

3. Beware of phishing and scams

Be **cautious of unsolicited** messages, links, or requests from unknown individuals on social media. **Avoid clicking on suspicious links** or downloading attachments from unknown sources, as they may lead to phishing scams or malware infections.



Tips

Many social media scams happen through the hacking of one of your contacts' account. Be cautious when a contact you know sends you unsolicited, unusual requests (such as financial support for their relatives in the hospital), and verify with them through another media)

4. Be mindful of location sharing and of what you post

Limit location sharing on social media platforms, especially when posting photos or updates in real-time. Avoid disclosing your exact location or sharing personal information that could compromise your safety or security.



Tips

Many types of information can be used by cybercriminals to cause harm. Aside from the obvious (name, age, gender, city of residence, etc.), many details can be used by cybercriminals, such as name of closest schools, former or current workplace, screenshots with personal data, etc.

4. Best practices and good habits



4.4. Social media and messaging

Safely use social media by integrating the following practices.

5. Verify account authenticity

Be wary of **fake or impersonated accounts** on social media platforms, especially those impersonating celebrities, public figures, or brands. **Verify the authenticity** of accounts before interacting with them or sharing personal information.



Tips

In 2021 alone, Facebook removed 1.7 billion fake accounts. Likewise, almost 1 out of 5 (19.42%) Twitter handles are fake or spam. The blue tick “certifying” an account can be earned by virtually anyone, and is not an indicator that an account can be trusted.

6. Monitor third-party apps and permission

Regularly **review and manage** the permissions granted to third-party apps connected to your social media accounts. Remove access for apps that you no longer use or trust to minimize the risk of data misuse or privacy breaches.



Tips

Pay attention to the permissions given to these applications because they could give access to private information that they shouldn't be privy to.

4. Best practices and good habits

4.5. Mobile device security

Use your **mobile device** more **safely** by integrating the following practices.

1. Use a secure screen lock
2. Keep your software and OS updated
3. Encrypt data
4. Use a trusted app store
5. Review app permissions
6. Be cautious of public Wifi
7. Enable “Find my device”
8. Limit use of Bluetooth and NFC

4. Best practices and good habits



4.5. Mobile device security

Use your **mobile device** more **safely** by integrating the following practices.

1. Use a secure screen lock

Enable a **secure screen lock** (e.g., PIN, password, pattern, biometric identification) to prevent unauthorized access to your device if it's lost or stolen. Avoid using easily guessable patterns or PINs.

3. Encrypt data

Enable encryption for data stored on your mobile device to protect sensitive information. Most modern mobile devices offer built-in encryption features that encrypt data at rest.

2. Keep your software and OS updated

Regularly **update your mobile operating system**, apps, and security patches to protect against known vulnerabilities and security threats. Enable automatic updates to ensure timely security patches.

4. Use a trusted app store

Download apps only from **official and trusted app stores**, such as the Apple App Store or Google Play Store, to minimize the risk of downloading malicious apps or malware.

4. Best practices and good habits



4.5. Mobile device security

Use your **mobile device** more **safely** by integrating the following practices.

5. Review app permissions

Review and manage app permissions to control what data and features apps can access on your device. **Disable unnecessary permissions** that apps don't require for their functionality.

7. Enable "Find my device"

Enable the "**Find My Device**" or "**Find My iPhone**" feature on your mobile device to remotely locate, lock, or erase your device in case it's lost or stolen. This feature helps protect your data and privacy in case of theft or loss.

6. Be cautious of public Wifi

Avoid connecting to **unsecured public Wi-Fi networks**, as they may be vulnerable to eavesdropping or man-in-the-middle attacks. **Use a VPN** to encrypt your internet traffic when connecting to public Wi-Fi networks.

8. Limit use of Bluetooth and NFC

Disable Bluetooth and NFC when not in use to prevent unauthorized access or pairing with other devices. Be cautious when pairing with unknown devices and use Bluetooth devices from trusted sources.

4. Best practices and good habits



4.6. Password security

Securitize your passwords by making sure they integrate the following elements.

1. Use strong and unique passwords
2. Use different passwords for each account
3. Use passphrases rather than words
4. Use a reputable password manager
5. Always keep passwords confidential
6. Regularly update passwords

4. Best practices and good habits

4.6. Password security

Securitize your passwords by making sure they integrate the following elements.

1. Use strong and unique passwords

Create strong, complex passwords that are difficult to guess. Use a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information such as names, birthdays, or common words.



Tips

Some sites give you an indication of the security of your password. Do not register a password until it is judged “strong” by the website or software. Passwords should have at least 16 characters and mix different types of characters.

2. Use different passwords for each account

Do not use the same password across multiple accounts. Use unique passwords for each online account to minimize the impact of a security breach on other accounts.



Tips

Use a password manager to prevent you from having to remember or write down passwords. You will only have to remember the password to your password manager.

4. Best practices and good habits

4.6. Password security

Securitize your passwords by making sure they integrate the following elements.

3. Use passphrases rather than words

Consider using **passphrases** instead of traditional passwords. Passphrases are longer **combinations of words or phrases** that are easier to remember but harder to crack. For example, "Icàre@b0utSecur1ty!" is a strong passphrase.



Tips

First choose a passphrase you can easily remember. Then establish your own “encryption system”, for example: o=0, i=1, a=@, etc. Make sure to also integrate uppercase letters and special characters.

4. Use a reputable password manager

Use a **reputable password manager** to securely store and manage your passwords. Password managers generate strong, unique passwords for each account and store them in an encrypted vault, accessible only with a master password.



Tips

Examples of reputable password manager are provided in the last section of this curriculum. Make sure to use the password generation feature to benefit from unique, strong and randomly generated passwords you do not have to remember.

4. Best practices and good habits

4.6. Password security

Securitize your passwords by making sure they integrate the following elements.

5. Always keep passwords confidential

Never share your passwords with anyone, including friends, family members, or colleagues. Keep your passwords confidential and avoid writing them down or storing them in easily accessible locations. Make sure to store them on a password manager.



Tips

If sharing a password is inevitable, best do so orally, or alternatively via a secure, encrypted application (ex: never on social media messaging channel). Do never share the login / email address via the same application, and do so via another media.

6. Regularly update passwords

Regularly update your passwords for online accounts, especially for sensitive accounts such as banking, email, or social media accounts. Change passwords immediately if you suspect they may have been compromised and let the password manager generate new ones regularly.



Tips

Remember to change default passwords that come with devices, routers, or software applications. Default passwords are often easy to guess and widely known, making them vulnerable to unauthorized access.

5. Useful tools and additional resources

1. Password managers
2. 2FA tools
3. Anti malwares
4. Encryption tools
5. Other tools

5. Useful tools and additional resources



5.1. Password managers



Password managers **securely store and manage passwords** across various accounts, simplifying access while ensuring strong, unique password creation and secure access. Make sure to:

- **Choose a strong, unique, memorable master password** – giving you access to the password manager. Be sure to remember it and never communicate it ; it is the door to all your accounts.
- **Let the password manager generate strong, unique passwords** for each of your accounts. It will remember and store them, and you will never have the same password twice.

5. Useful tools and additional resources



5.2. Two-factor authentication (2FA) tools



Two-factor authentication (2FA) tools increase an account's security by forcing the user to validate his log-in on two different, registered and trusted devices, usually on the phone and the computer.

5. Useful tools and additional resources



5.3. Anti-malwares



Anti-malwares or anti-viruses identify and remove various malware types, providing real-time protection against cyber threats for devices and networks.

5. Useful tools and additional resources

5.4. Encryption tools



Encryption tools create encrypted containers, safeguarding sensitive files and folders by preventing unauthorized access through encryption. Some tools, such as Bitlocker encrypt external peripherals like hard drive to enhance their security.

5. Useful tools and additional resources



5.5. Other useful tools

Name	Type	Description
PRIVACY BADGER	Browser Extension	Privacy Badger blocks tracking cookies and ads, safeguarding user privacy by preventing third-party trackers from collecting browsing data.
IMPRIVATA	Access Management	Imprivata offers single sign-on solutions, allowing care professionals to access multiple applications securely with a single login, streamlining workflow without compromising security.
HIPAA ONE	Compliance Tool	HIPAA One automates HIPAA compliance, aiding healthcare organizations in meeting regulatory requirements, conducting risk assessments, and ensuring data security.
SYMANTEC ENDPOINT PROTECTION	Endpoint Security	Symantec Endpoint Protection offers comprehensive security, including advanced threat protection, antivirus, and firewall features, safeguarding against cyber threats in healthcare environments.
TEAMVIEWER	Remote Desktop Access	TeamViewer allows remote access and control of devices, aiding remote technical support, troubleshooting, and collaboration across locations.
CISCO ANYCONNECT	VPN Tool	Cisco AnyConnect provides secure VPN connections, allowing encrypted access to organizational networks from remote locations, safeguarding data transmissions.
ADOBE SIGN	E-Signature Platform	Adobe Sign facilitates secure digital document signing, simplifying and expediting the signing process, ensuring compliance and security in document management.

Thank you for your participation and ideas!

