



ASTeK
IMS

Information's security awareness Common Core Module

François FEVRIER – CISO – ffevrier@groupeastek.fr

GENERAL INFORMATION ABOUT IS AND SECURITY

THREATS AND ATTACKS

BEST PRACTICES

SYNTHESIS

WHAT IS AN INFORMATION SYSTEM ?

An Information System (IS) makes it possible to **collect, store** and **process** information in various formats in order to deliver it to the right person at the right time in the appropriate format.



The IS must be seen as a set of resources:

- Human
- Material
- Immaterial

As the world is becoming hyperconnected, **IS are present everywhere**, whether in the professional or personal environment, **in various forms**.

The material resources of an IS don't only include computers or network equipments but all connected objects, grouped under one term: **Internet of Things (IoT)**.

Some examples:

- Printers
- Cameras
- Cell phones
- Connected watches



CONFIDENTIALITY

The data is restricted to authorized persons only.

INTEGRITY

The data is not altered intentionally or accidentally during processing, storage and exchange.

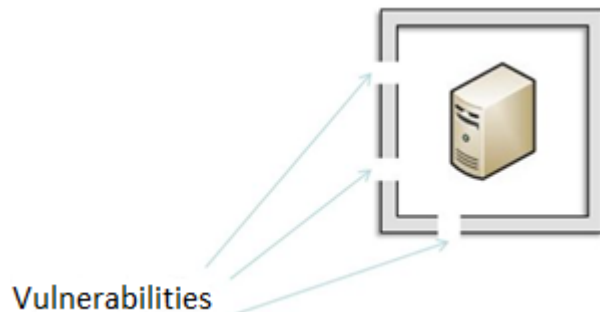
AVAILABILITY

Access to services and resources must be maintained.

TRACEABILITY

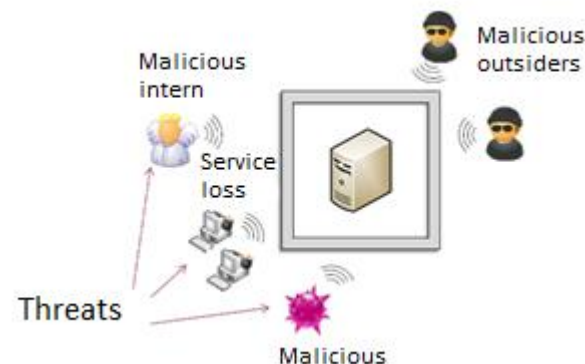
The author cannot deny his involvement.

Vulnerability



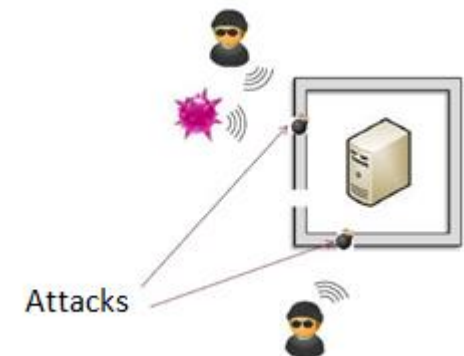
Weakness in an asset (in the design, execution, installation, configuration or use of the asset).

Threat



A potential cause of an incident that could result in damage to an asset if the threat becomes a reality.

Attack



Malicious action designed to compromise the security of an asset. An attack represents the realization of a threat and requires the exploitation of a vulnerability.

GENERAL INFORMATION ABOUT IS AND SECURITY

THREATS AND ATTACKS

BEST PRACTICES

SYNTHESIS

THREATS

Threats &
attacks

Increasingly frequent and diverse threats



States



Criminal groups



NETWALKER



Competitors

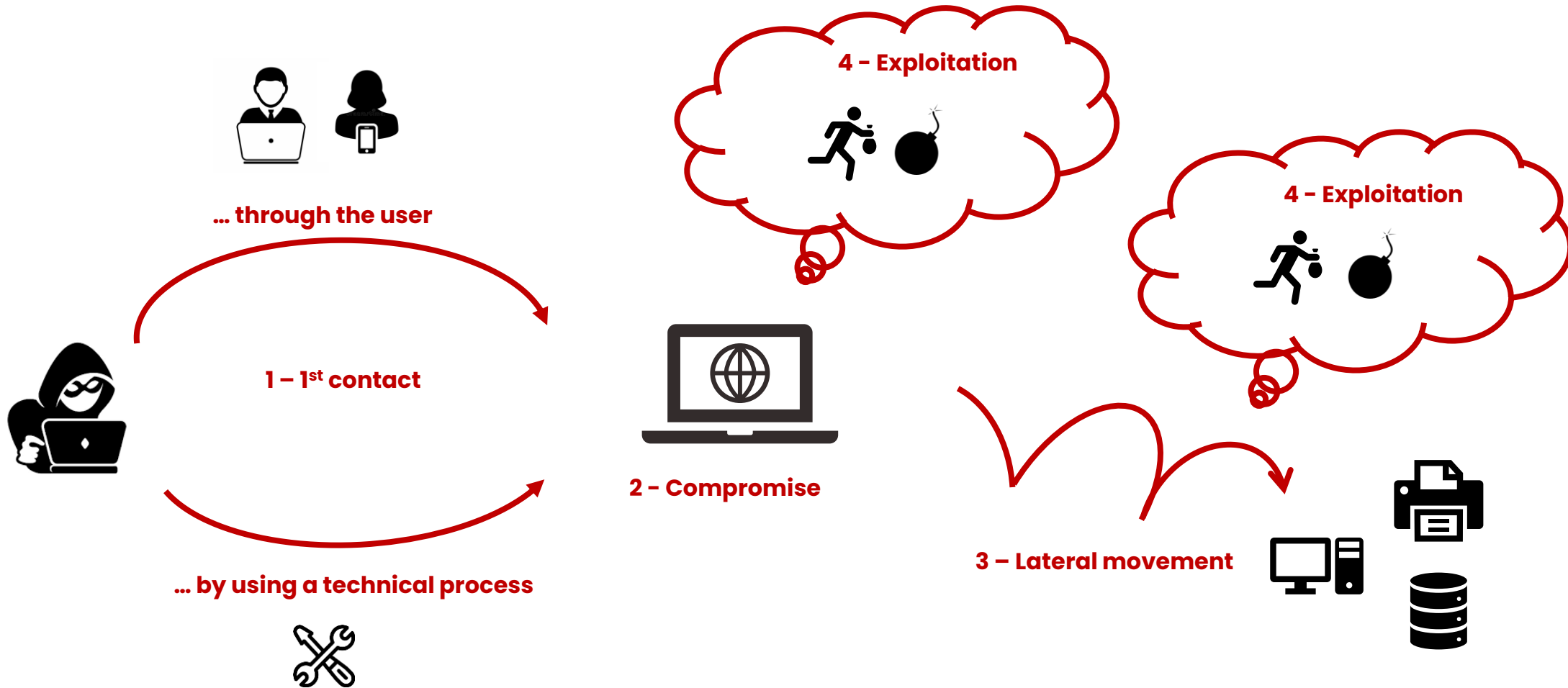


Activistes



TYPICAL ATTACK PROCESS

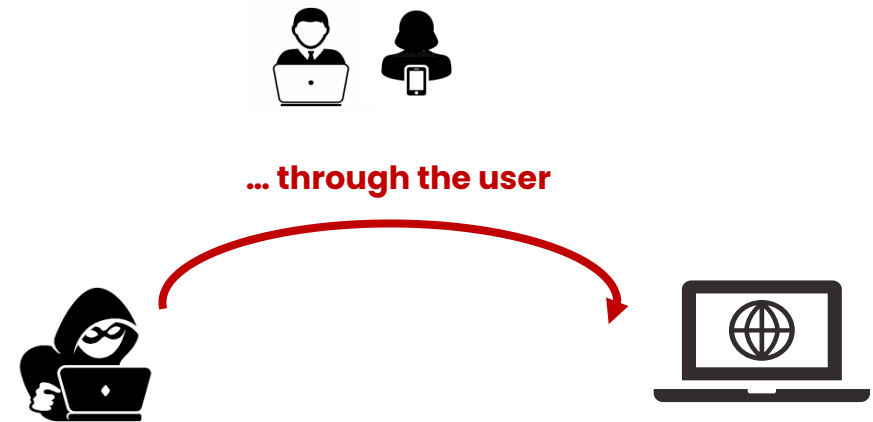
Overall stages of an attack



The user as a target for social engineering attacks

Fooling someone is a simple and effective way to bypass the initial security set up without raising doubts.

The use of social engineering allows to **quickly gain the trust of victims** in order to convince them to do certain actions (click on links, provide confidential information). Emotions such as fear, curiosity, kindness or urgency are targeted.



Social engineering:



Targeted : target survey



Massive : using corporate codes¹

Attack vectors:

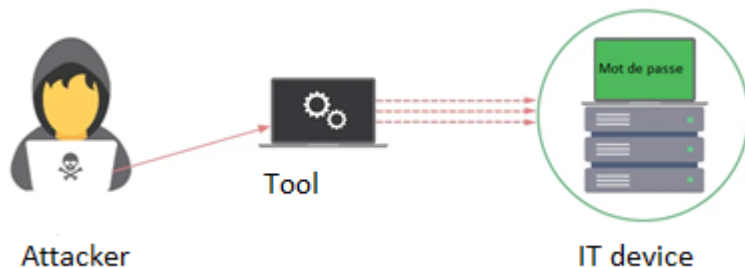
- Emails (phishing)
- SMS (phishing)
- Phone calls (president scam)
- Brute force attack on passwords

¹: common language or method of communication specific to the company.

Focus on the most common initial attack vectors

Brute Force

Attack to **crack a password** or any user authentication mechanism



Social engineering:

Manipulative technique to get people to reveal confidential information



Phishing



Fraudulent technique designed to **fool the user** into giving out personal data (access accounts, passwords, etc.) and/or banking data by pretending to be a trusted third party

Technical vulnerabilities exploitation : complex but powerful

The attacker will try to **gain access to the device** by using vulnerabilities in :

- Network
- Servers
- Applications
- Protocols



1 – 1st contact



... by using a technical process



The compromise

An IS object is defined as **compromised if it can no longer be considered secure**: it no longer really belongs to you. The compromise can concern anything: a computer, a server, a smartphone or an application.

This will result in the **introduction of malware** into the infected system.



2. Compromise



A compromised system is **equivalent to a stranger having a spare key to your home.**

Focus on malware

Rootkit :

malicious software that gives a hacker remote access into your device

Worm :

stand-alone malicious software capable of replicating and spreading through computer networks

Ransomware:

malicious software that blocks access to the computer or files by encrypting them and then demands that the victim pay a ransom to regain access (example: WannaCry)

Trojan :

software that appears to be legitimate but contains malicious features.

Spyware :

spyware that infects your computer or mobile device and collects information about you (files, photos, contacts, microphone, camera ...)

Adware :

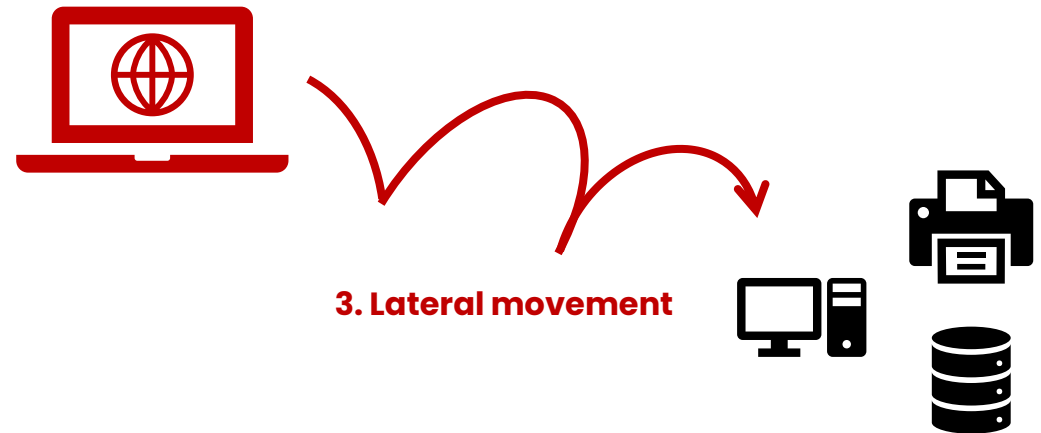
malware designed to display pop-up ads on your screen

MALWARE



Lateral movement

The principle of lateral movement is to **use a compromised system as a relay** to get access to a maximum number of devices.



Example:

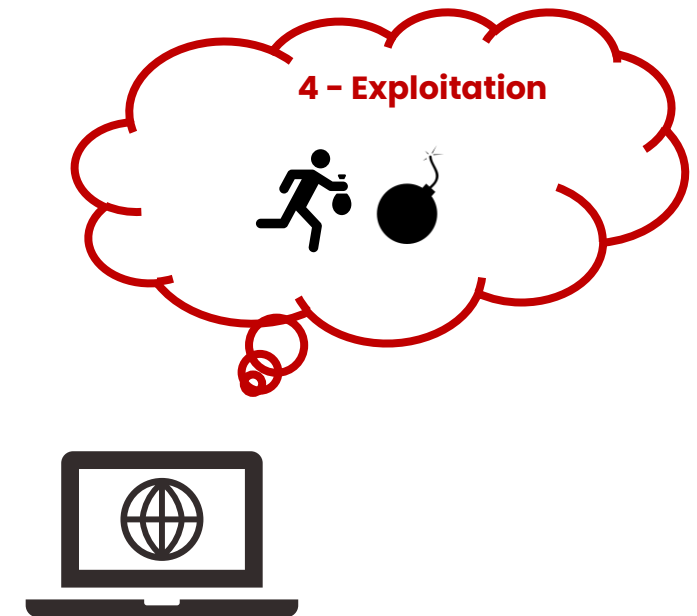
Compromised email addresses lead to more powerful phishing and therefore more material to infect.

Consequences

Like a disease, once the attack has had time to incubate with the previous steps, the signs show.

In our interconnected world, this can be :

- **Theft** of confidential data
- **Spying**
- Sabotage (often for **ransom**)
- Use of our machines to provide **illegal services**



GENERAL INFORMATION ABOUT IS AND SECURITY

THREATS AND ATTACKS

BEST PRACTICES

SYNTHESIS

Selecting a password

A strong password is :

- A password of at least **12 characters**
- With **different types of characters** (upper case, lower case, numbers, special characters)
- A password that has **no connection with you** (name, date of birth, etc.) and is not in a dictionary.

And nevertheless, the most used passwords are still 123456, password, picture1, sun,

Example of **bad passwords** that might be used **internally** :

- astek1234
- astek2021
- Intitek123

Top worst passwords of the year 2020

Position	Password
1. ↑ (2)	123456
2. ↑ (3)	123456789
3. (new)	picture1
4. ↑ (5)	password
5. ↑ (6)	12345678
6. ↑ (17)	111111
7. ↑ (18)	123123
8. ↓ (1)	12345
9. ↑ (11)	1234567890
10. (new)	senha
11. ↑ (12)	1234567

Consequences of reusing passwords



A **password** must be **unique** to each service /application.



Mary Smith
msmith@groupeastek.com + msmith@gmail.com



Password ≥ 12 characters: r&4vvq*Hd|2g2t



Mary underestimates the importance of using unique passwords



Instagram data leak



The attacker downloads the passwords

BREAKING NEWS

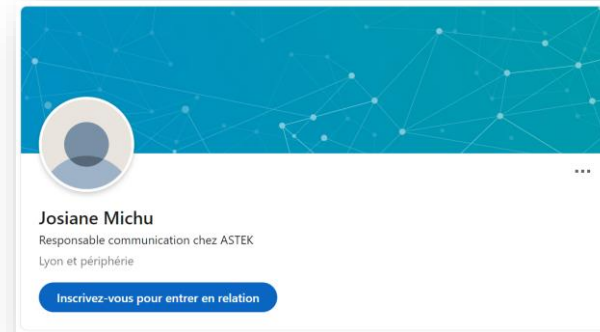
Consequences of reusing passwords



A **password** must be **unique** to each service /application.



Investigate



Attacker:

- Knows that Mary SMITH works for ASTEK
- Knows the format of ASTEK's email addresses

Consequences of reusing passwords



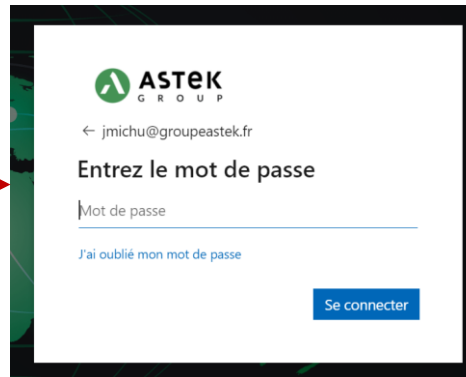
A **password** must be **unique** to each service /application.



When
investigating the
attacker



sees that ASTEK
uses Office 365



Attacker uses
leaked



Instagram
password



By reusing her leaked Instagram password as a session password, Mary Smith allowed an attacker to compromise an ASTEK account.

How to have only strong and unique passwords?

Re-using passwords is like re-using your house key for all locks !

Tools exist to avoid remembering them, only **ONE** will remain in your memory: the one to connect to the **password manager** !



Password managers allow you to:

- **Store** all your passwords
- **Generate** your passwords
- **No more worries about remembering** all your passwords

Keeping its services up to date

This concerns:

- Operating system
- Browser
- Antivirus
- Application
- Software
- ...



Updates not only bring new features but also **security patches**.

Perfect security does not exist, but not updating means more exposure to threats unnecessarily.

Be careful with your smartphone/tablet

Connected objects (IoT) are everywhere and you have to be as careful with them as with a computer.

Tips:

- Be aware of the applications you install
- **Keep only useful applications,** old applications could be a source of vulnerabilities
- Don't forget that it is a mine of sensitive information
- **Report** lost or stolen devices to the IT department quickly.



Internet browsing rules

The Internet is a dark street full of strangers! Danger can be hidden behind a link, a file or even a button (which is ultimately a link).

Best practices:

- Always **download** software from **official websites**
- Do not accept **cookies** by default.
- **Do not save passwords by default**
- Be careful about the sites you access
- Pay attention to installed add-ons.
- **Disconnect** from applications before closing your browser



What is HTTPS?



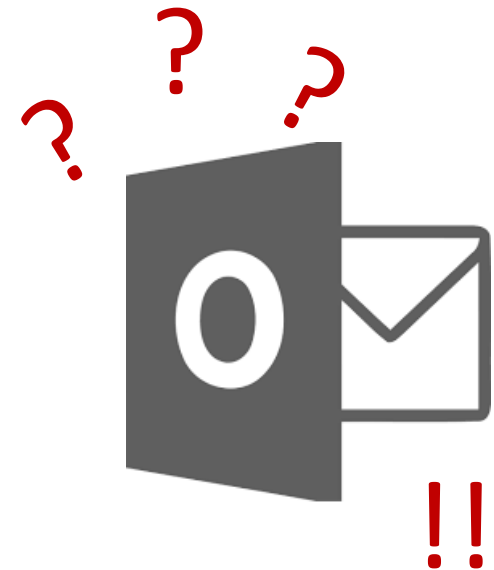
An https website ensures that the connection between the web browser and the web server is **encrypted with a trusted certificate** but does not ensure that the website is reliable. For any download or purchase it is recommended to use **platforms that are trusted** in order to avoid unpleasant surprises.

The use of email

E-mails and attachments are often central to the process of a computer attack.

Steps :

- **Check the sender's email address** carefully
- The presence of **grammatical errors** can be a warning
- **Never click directly on a link**, hovering over it with your cursor will display its exact URL
- Never reply to an email that requests personal or confidential information
- **Do not open attachments from unknown** and/or suspicious sources
- Do not forward false information, hoaxes, or any other spam / scam



It is important to keep a critical eye even for senders you know. It may be possible that their addresses have been corrupted without them knowing it. **Never trust the name of the sender when it appears.**

The use of email

So.... Phishing or not Phishing

From: Microsoft office365 Team [<mailto:cyh11241@lausd.net>]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your email account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

[Verify Now](#)

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

The use of email

So.... Phishing or not Phishing → **Yes Sir !**

**The sender's
e-mail
address**

refers to a
different
domain
name :
lausd.net

From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your email account will be blocked.

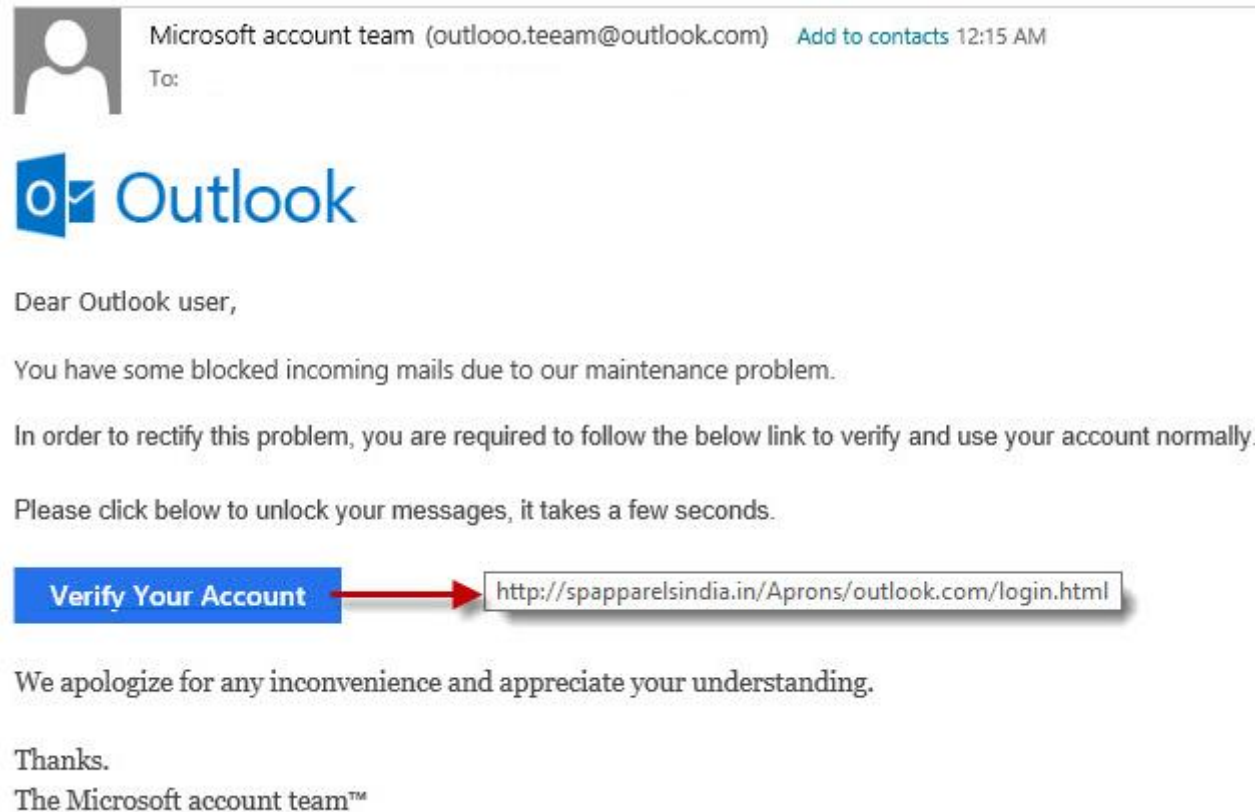
If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

[Verify Now](#)

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

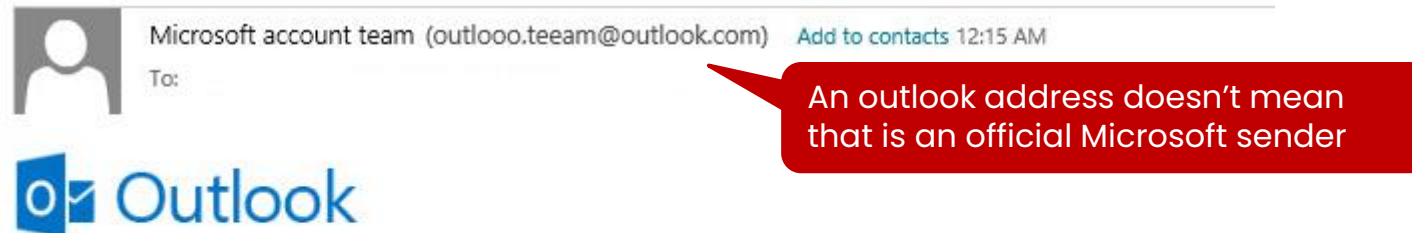
The use of email

So.... Phishing or not Phishing ?



The use of email

So.... Phishing or not Phishing ? ➔ **Yes Sir !**



Microsoft account team (outlooo.teeam@outlook.com) Add to contacts 12:15 AM
To:

Outlook

Dear Outlook user,

You have some blocked incoming mails due to our maintenance problem.

In order to rectify this problem, you are required to follow the below link to verify and use your account normally.

Please click below to unlock your messages, it takes a few seconds.

Verify Your Account ➔ <http://spapparelsindia.in/Aprons/outlook.com/login.html>

We apologize for any inconvenience and appreciate your understanding.

Thanks.
The Microsoft account team™

An outlook address doesn't mean that is an official Microsoft sender

When hovering (without clicking) the mouse over the link, you will notice that the **link does not redirect** to the office365 website

Separate business and personal use

The security and uses are not the same on a personal and professional device, especially for communications.

Basic recommendations:

- **Do not forward business messages** to personal email accounts
- **Do not store** business data on personal storage media
- **Do not connect** external storage media



It is important to keep in mind that the security of a personal device is often weaker because it is not subject to company policy. This makes it a more vulnerable vector for an attacker.

Controlling the spread of information

The amount of **personal/professional information that ends up online must be limited**. Once the information is on the Internet, it becomes accessible to everyone.

Attention to:

- The **forms** to be filled in
- Restrict access to personal information on **social networks** as much as possible.
- **Use different email addresses** according to the sensitivity of the activities.
- Be careful with sites that are too curious
- Avoid linking accounts by authenticating with Google for example.
- The cloud, websites, applications, etc. are subject to data leakage that can be made public.



The website **<https://haveibeenpwned.com/>** allows you to find out if one of your email addresses is part of a known data leak.

Physical security

A proximity attack can be made when travelling on business or working in a place with other people.

Rules to follow:

- **Lock** your equipment when not in use
- Do not leave equipment **alone**
- Do not write sensitive information **on paper** (especially passwords)
- Do not travel with more sensitive information than you need to carry
- Beware of **intrusive eyes** and cameras
- **Use two-factor authentication** as much as possible.



As a reminder, we are not only talking about computers, but also about smartphones and tablets, to mention just a few.

GENERAL INFORMATION ABOUT IS AND SECURITY

THREATS AND ATTACKS

BEST PRACTICES

SYNTHESIS

Attack on the IS

Attacks on our IS are a daily event.

Human factor

The biggest attack vector is through people.

Password

A password must be random and at least 12 characters long

Update

Keep your devices up to date

Phishing

Suspicious mail: do not open attachments, do not click on links

In case of any doubt

Please contact:
securite@groupeastek.fr



ASTEK

Thank you for your attention