CYBERYOUTH

Non-formal education for cyber-security training & resilience of youth organisations and young people

Secure System Architecture and Design

Session Activity 1

Zombie Computer

Co-funded by the European Union

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.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

In this session, you will learn how to prevent your computer and devices from becoming a zombie device.

CYBERYOUTH

Co-funded by the European Union

Do you believe in Zombies? (little energizer activity)

- Do you think zombies exist?

- People use the word “zombie” a lot more loosely — often metaphorically — to refer to anyone or anything that presents as apathetic, moves slowly, and demonstrates little awareness of their surroundings.

- Why do you think people watch Zombi movies and play Zombie games a lot?

- Can humans ever become zombie-like?

- If one day Zombies existed, what would be your reaction? Kill it directly or try to rehabilatate them?

CYBERYOUTH

Co-funded by the European Union

Zombie Computer

- “Zombie” is the term used when an attacker takes control of your computer without your knowledge. A zombie attack aimed either to steal your sensitive information or to make your computer do things that it normally shouldn’t. For example, a hacker could use your device to send out spam or, even worse, to attack other computers or IT systems. Worry it might happen to you?

Co-funded by the European Union

What is a Zombie Computer?

- A zombie computer is the result of a cyber-attack similar to a traditional Trojan Horse attack (a malicious code wrapped inside a regular behaving code). But instead of aiming only to install a keylogger and steal your personal data, the malicious software will transform your computer into a zombie: thanks to this infection, the hackers can control it remotely. Very often, they will make it “work” with other zombies. Together, all these infected computers will form a botnet (or a zombie army).

CYBERYOUTH

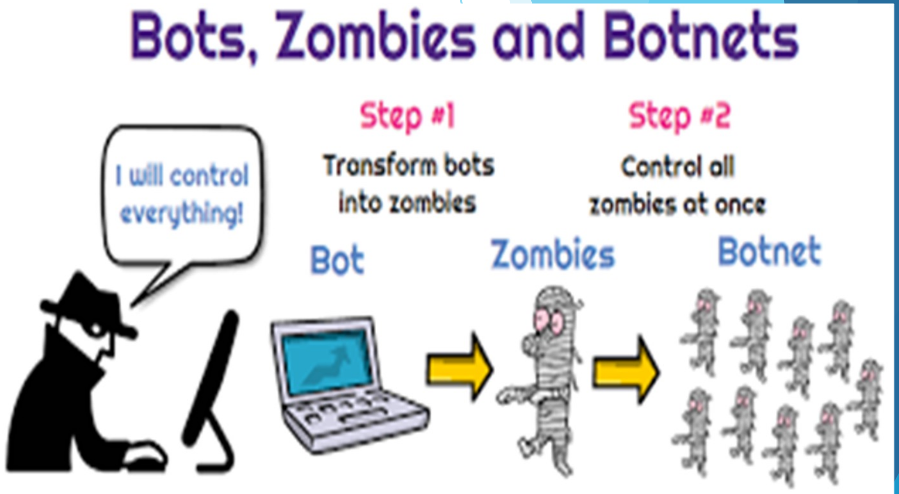
Co-funded by
the European Union

BOTNETS

Botnets

The term botnet is a portmanteau word made with the terms ‘robot‘ and ‘network’. Botnets are entire networks of computers controlled and instructed to do many kinds of hostile things, such as:

- ▶Attack other computers (for example DDoS attacks)
- ▶Send spam or phishing emails
- ▶Infect other computers or IT systems with malware (ex. ransomware, spyware,…)
- ▶Commit advertising frauds
- ▶Other similar malicious acts…
- ▶The worst part is that it all can happen without you having the slightest idea about it. J))


Bots, Zombies and Botnets
I will control everything!
Step #1
Transform bots into zombies
Step #2
Control all zombies at once
Bot
Zombies
Botnet

CYBERYOUTH

Co-funded by the European Union

How can my computer turn into a zombie?

►It only takes malware to turn your computer into a zombie. Malware is a virus or malicious software insidiously installed on your computer. Once your computer is infected, this program runs to perform unwanted actions that are often harmful to you.

►Hackers have several options for infecting a computer with malware. They can use a loophole in software or firmware that has not been updated to introduce it into an organization’s computer system or an individual’s computer or embed it in a misleading email. All it takes is a browser plugin update you just keep postponing or a click on a link in an email that seemed to come from a trusted institution.

►The bad news is that smart cybercriminals are now using encryption to bypass the conventional virus scanning and spamming checks – making malware (almost) undetectable.

Co-funded by
the European Union

What are the signs my computer is now a zombie?

Here are some clues your device may have been infected by malware and consequently turned into a zombie :

- A part of your hard disk or flash storage **seems to have disappeared**.
- Your browser **often closes** for no apparent reason.
- Inexplicable error messages **pop out randomly**.
- Your computer **takes a long time** to start up and shut down.
- Your **fan is going into overdrive** even though your PC is supposed to be idle.
- There are emails in your “Sent” folder **you don’t remember writing**.
- Some **security websites block you** from accessing them.
- You can’t **download or install antivirus programs** or updates.
- Windows Task manager shows **suspicious programs** you can’t account for.
- If you can relate to one or more of these assumptions, there’s a *slight possibility* that your computer has become a zombie.

CYBERYOUTH

Co-funded by the European Union

What can I do if my computer has become a zombie?

►The first thing to do to try to recover your computer from a zombie attack is to run a scan of your antivirus. You'll have to install an antivirus if you don't have one. You can then run a scan of your entire system to detect any potential malware.

►Very often, if your antivirus finds some virus or malware, it will suggest to you some steps to get rid of it. We advise you to follow them carefully. In many cases, it'll manage to get rid of the problem, and you'll recover your computer.

►But sometimes, it won't work and your antivirus will prove unable to remove the malware. In this case, you can only erase your computer's hard drive(s) and reinstall your operating system and software.

►In this scenario, you will lose all the data that has not been backed up. This highlights the importance of regular and comprehensive backups.

CYBERYOUTH

Co-funded by
the European Union

How can I prevent my computer from becoming a zombie?

►Most cyberattacks (91%) are initiated with a phishing email. It means following secure email practices is essential to help you prevent your device from becoming a zombie. These are the following :

►Don’t click on any suspicious link you’re not sure of / or don’t know where it leads – not even the ones you received from friends, family, or social network buddies. Their accounts might have been compromised. It’s safer to be patient and ask them what it’s all about before rushing to click on the link.

►Do not download any attachments that you never requested.

►Avoid opening spam messages. Especially, don’t click on links that say ‘click here to unsubscribe/etc.’ as they will mostly do the opposite (run a malicious program, …)

►Beware of browser plugins/add-ons and non-trusted apps and avoid giving them unnecessary permissions.

►Install mobile apps with extreme caution– and avoid clicking on fancy ads that normally lead you to watering holes using malvertising. Don’t use pirated, cracked, or otherwise illegal copies of programs. Only download them from trusted sources.

►Pay much attention when opening content from encrypted emails, as encryption could hide malicious content.

CYBERYOUTH

Co-funded by the European Union

QUIZ

1) A collection of zombie computers have been set up to collect personal information. Which type of malware do the zombie computers represent?

a) Spyware

b) Trojan horse

c) Botnets

d) Logic bomb

2) What is the process of encoding information in a way so that only someone with a key can decode it?

a. Compression

b. Systemic variation

c. Encryption

1) What is a firewall?

a. An antivirus software

b. Software that logs Internet activity

c. A filter for an Internet connection

CYBERYOUTH

Co-funded by the European Union

QUIZ

4) Which kind of malware typically resides in a larger, innocent computer program?

a. Worm

b. Trojan horse

c. Computer virüs

Answers:

1) C
2) C
3) C
4) C

CYBERYOUTH

Co-funded by
the European Union

THANK YOU!

CYBERYOUTH

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.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by
the European Union

CYBERYOUTH
Non-formal education for cyber-security training & resilience of youth organisations and young people

Secure System Architecture and Design

Session Activity 2

Social Engineering

Co-funded by the European Union

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.

Project No: 2021-1-IT03-KA220-YOU-000028668

Welcome!

In this session, you will learn about what is social engineering, its attack cycle, common social engineering attacks and more.

CYBERYOUTH

Co-funded by the European Union

Little Energizer

- Do you think you are easily manipulated or not? it can be political manipulation, cultural, linguistic or any type?
- Do you think you manipulate things when you needed?

Do you have any experience\story to share?

CYBERYOUTH

Co-funded by
the European Union

SOCIAL ENGINEERING

Social Engineering is the art of manipulating people so that they give up confidential information or break standard security practices.

CYBERYOUTH

Co-funded by
the European Union

Facts About Social Engineering

Everyone is a potential target!

It's often easier for cybercriminals to manipulate a human than a computer network or system.

Attacks can be relatively low-tech, low-cost, and easy to execute.

Technology is rapidly accelerating along with the sophistication of attacks.

CYBERYOUTH

Co-funded by the European Union

Common Social Engineering Attacks

- Pretexting
- Phishing/Spear Phishing
- Vishing
- Smishing
- Baiting
- Scareware
- Ransomware
- Dumpster Diving
- Shoulder Surfing

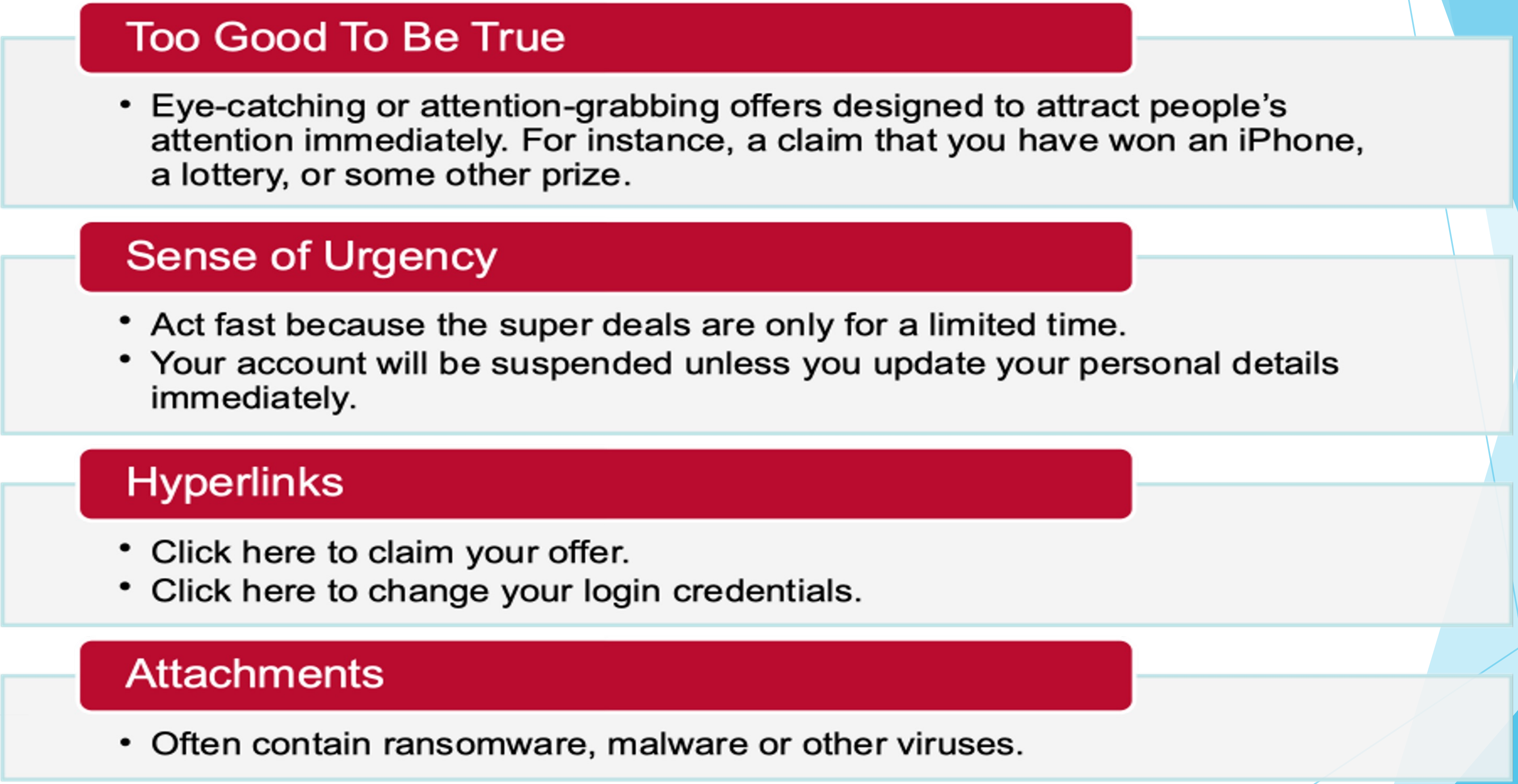
Co-funded by
the European Union

Phishing

A type of attack often used to steal user data, including login credentials, personally identifiable information or credit card numbers. It occurs when an attacker poses as a trusted entity, dupes a victim into opening an email or instant message.

Co-funded by the European Union

Common Signs of Phishing



Too Good To Be True

- Eye-catching or attention-grabbing offers designed to attract people’s attention immediately. For instance, a claim that you have won an iPhone, a lottery, or some other prize.

Sense of Urgency

- Act fast because the super deals are only for a limited time.
- Your account will be suspended unless you update your personal details immediately.

Hyperlinks

- Click here to claim your offer.
- Click here to change your login credentials.

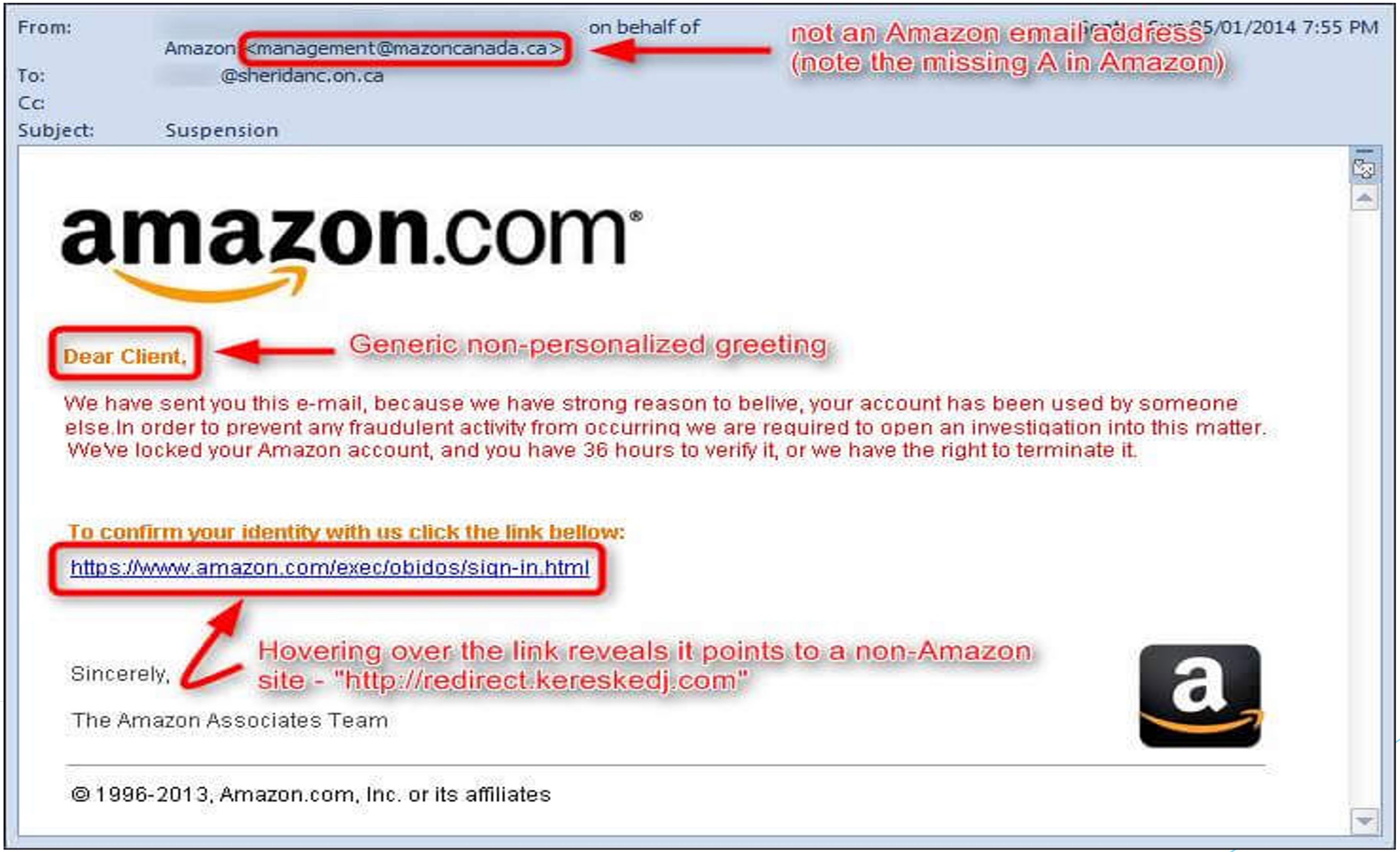
Attachments

- Often contain ransomware, malware or other viruses.

CYBERYOUTH

Co-funded by
the European Union

Phishing Email



From: [redacted] on behalf of Amazon <management@mazoncanada.ca> 5/01/2014 7:55 PM

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

CYBERYOUTH

Co-funded by the European Union

Other Forms of Phishing

Spear Phishing

- Similar to phishing, spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

Vishing (Voice Phishing)

- An attacker calls their target and uses an automated recording designed to generate fear. The recording will ask the target to call a number to resolve the issue.

Smishing (SMS Phishing)

- An attacker tries to trick you into giving them your private information by sending you a text message.

CYBERYOUTH

Co-funded by the European Union

THANK YOU!

CYBERYOUTH

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.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by
the European Union

CYBERYOUTH
Non-formal education for cyber-security training
& resilience of youth organisations and young people

Secure System Architecture and Design

Session Activity 3

Baiting

Co-funded by
the European Union

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.

Project No: 2021-1-IT03-KA220-YOU-000028668

What we will learn

Baiting techniques and how people become victim of fraud coming from various online resources.

CYBERYOUTH

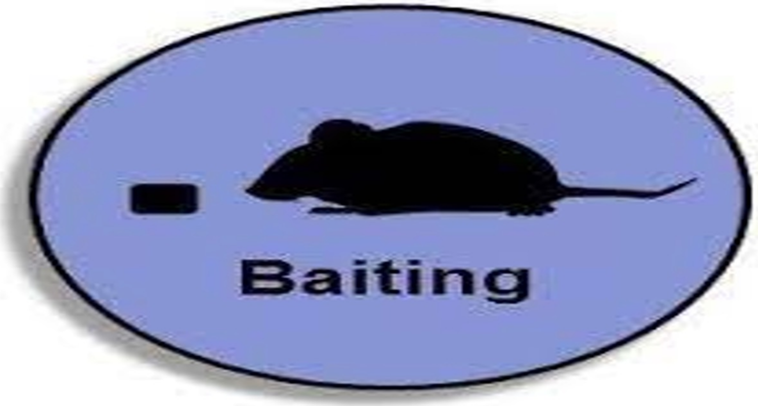
Co-funded by the European Union

Energizers

Did anyone catch any fish with bait?

What is Bait?

Can you think of anything as a bait to deceive people?



CYBERYOUTH

Co-funded by the European Union

What is Baiting?

Involves offering
mething physically
ligitally enticing to
arget in exchange
r login information
or private data.

CYBERYOUTH

Co-funded by the European Union

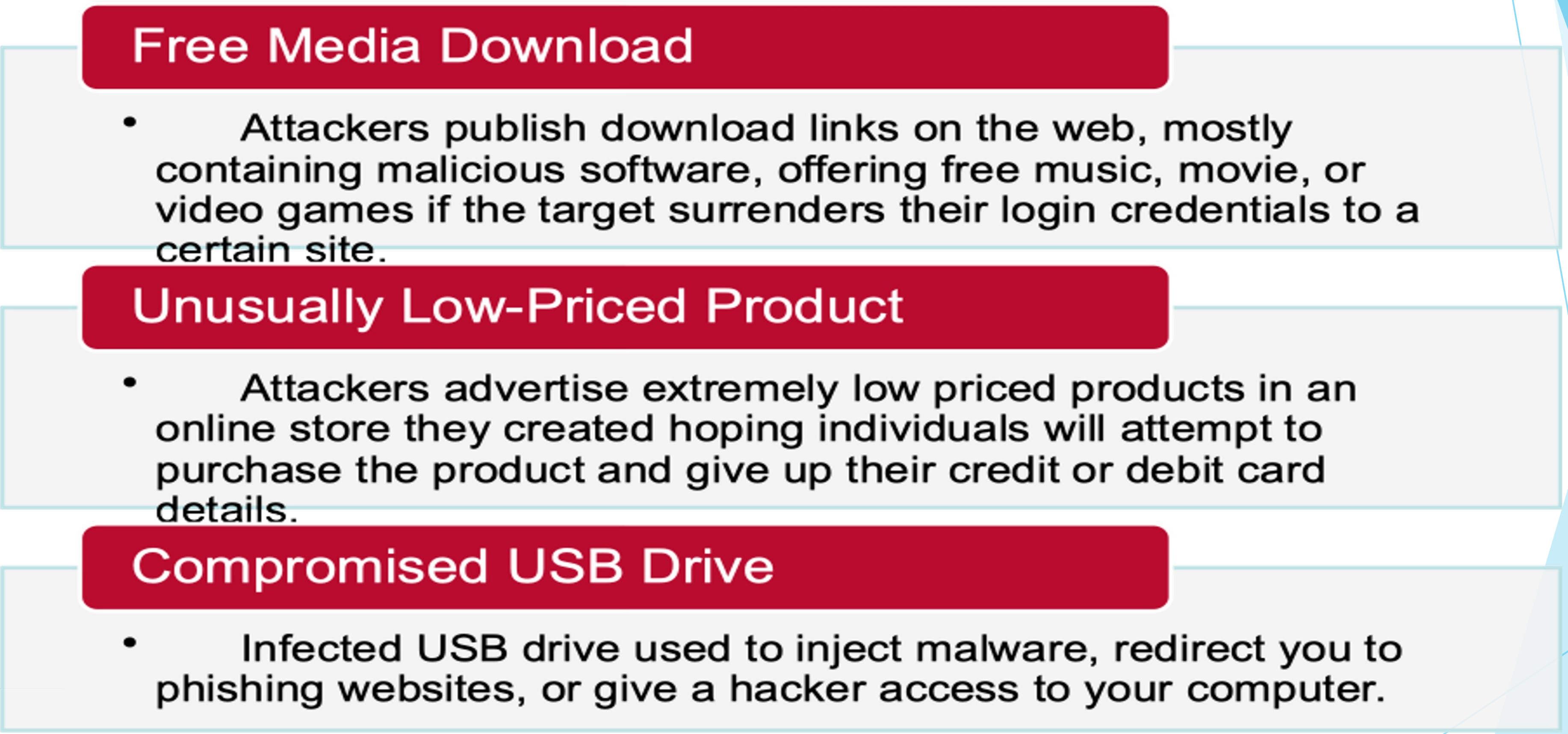
Baiting Techniques

Wells Fargo: Irregular activity on your account!
LinkedIn: Your account is at risk!
FEDEX: Sorry we missed you
FEDEX
FEDEX
FEDEX:
FEDEX
FEDEX
FEDEX!
FEDEX!
Rothstein / MORGAN 2020
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

CYBERYOUTH

Co-funded by the European Union

Baiting Techniques



Free Media Download

- Attackers publish download links on the web, mostly containing malicious software, offering free music, movie, or video games if the target surrenders their login credentials to a certain site.

Unusually Low-Priced Product

- Attackers advertise extremely low priced products in an online store they created hoping individuals will attempt to purchase the product and give up their credit or debit card details.

Compromised USB Drive

- Infected USB drive used to inject malware, redirect you to phishing websites, or give a hacker access to your computer.

CYBERYOUTH

Co-funded by
the European Union

Examples of Baiting Techniques

Examples of baits used by phishing to trick you

- Email and website spoofing. ...
- Malicious links and attachments. ...
- Urgent subjects and text lures. ...
- Identity forgery. ...
- Critical and timely subjects.

CYBERYOUTH

Co-funded by
the European Union

How To Prevent a Successful Baiting Attack?

- ## 1. Educate Your Staff

The first step to preventing a successful baiting attack is educating your employees on protecting themselves. This can be done through training and awareness campaigns, but keeping them up-to-date on the latest phishing trends and tactics is important. You should also teach them to recognize potential threats before clicking on any links or opening any attachments.

- ## 2. Don’t Follow Links Blindly

It’s easy for employees to get lazy and click on whatever link they see in an email because they assume that if someone sends it, it must be safe. However, this isn’t always true—phishers often send messages that look like they come from legitimate sources, such as your company’s email address or another employee’s address (such as someone who works in HR).

- ## 3. Educate Yourself To Avoid Baiting Attacks

Learn to think skeptically about any offer that’s too good to be true, such as an offer for free money or items.

The deal probably isn’t as good as it seems.

If someone asks you for personal or financial information over email or text, even if they claim they’re from your bank, don’t give it out! Instead, call your bank directly and ask if they sent the message asking for this info (and then report the scammer).

CYBERYOUTH

Co-funded by the European Union

How To Prevent a Successful Baiting Attack?

4. Use Antivirus and Anti-malware Software

Many good antivirus programs are available, but not all will protect you from a baiting attack. You need to ensure you have one that can detect and block the latest threats before they infect your computer. If you don’t have one installed, you can try out our free Malwarebytes Anti-Malware Premium software, which provides real-time protection against malware and other threats.

5. Don’t Use External Devices Before You Check Them for Malware.

External devices like USB flash drives and external hard drives can carry malware that can infect your computer when they’re connected. So make sure any external device you connect to your computer has been scanned for viruses first.

6. Hold Organized Simulated Attacks

Another way to prevent successful baiting attacks is by holding organized simulated attacks. These simulations help identify weaknesses in your systems and procedures, allowing you to fix them before they become real problems. They also help employees get used to identifying suspicious behavior, so they know what to look for when it happens.

CYBERYOUTH

Co-funded by
the European Union

USEFUL RESOURCES

Watch the youtube video about how to prevent a baiting attack

https://www.youtube.com/watch?v=oAKYWPK0LPs

Watch the youtube video about baiting attack awareness

https://www.youtube.com/watch?v=x7vcVsUNC-Y

CYBERYOUTH

Co-funded by the European Union

THANK YOU!

CYBERYOUTH

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.

Project No: 2021-1-IT03-KA220-YOU-000028668

Co-funded by
the European Union