Erasmus+ Programme – Strategic Partnership
Project Nr 2020-1-RO01-KA229-080232_1

Erasmus+ project, KA229, "EmotionsMapping/EMap"

Safer Internet Day /E-Safety Day , SID, 08.02.2022

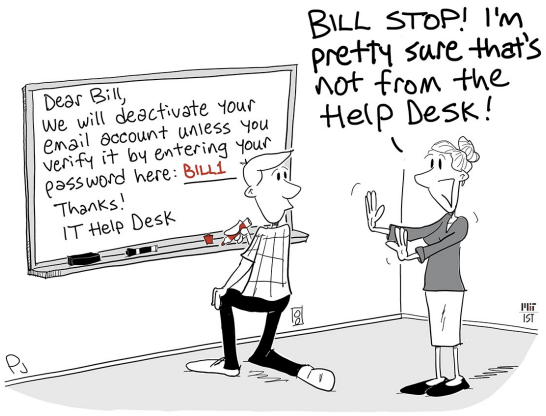
saferinternetday.org

What is phising?

https://www.youtube.com/watch?v=BnmneAjVrM4

It can also occur through SMS messages on mobile devices – commonly referred to as 'smishing'.

As the video above explained, the most common form of phishing is an email that appears to be from a reputable source such as your bank or an online service you use (such as Netflix). During periods of lockdown in 2020 these attacks increased significantly, particularly targeting home workers. However, young people can also be targeted by phishing scams. This report found that Microsoft, Facebook and PayPal were the three biggest online brands impersonated in phishing attacks in 2020. The UK's National Cyber Security Centre (NCSC) reported that it prevented 15,354 campaigns that has used Covid-19 as a theme throughout 2020.



https://chumworth.medium.com/beware-of-all-phishing-attempts-882c3fec15ad

How can you spot a phishing attempt?

5 things to look for to spot a phishing email:

1. Sent from a public email domain – a message from a large genuine company will never be sent from an email address such as @gmail.com or @outlook.com.

2. Misspelt domain name – if the email domain is misspelt, or the website it links to contains a misspelt address then these could also be clues that they are not genuine. Some scammers will buy up misspelt web address that closely mimic genuine ones e.g. www.göögle.com as this can easily fool people who merely glance at the address rather than studying it in detail.
3. Poor grammar or spelling – these can be indications that the email isn't genuine. Poor grammar is often a better indicator as scammers will often use translation tools to translate their message into the required language, so spellings will be correct, but sentence structure might be poor and easily spotted by a native speaker.
4. Suspicious attachments or links – emails containing attachments or directing a recipient to click on a link are often hiding a piece of malicious software (malware). Files can easily be renamed to something that might tempt a recipient to open it e.g. 'invoice.pdf'.
5. A sense of urgency – emails that prompt the recipient to take immediate action, such as an urgent email from your boss asking you to send information, or a message that appears to be from an online service threatening to suspend your account, could be phishing attempts. Rushing recipients into taking action gives them less opportunity to examine the email closely and spot any clues that might give away a fake.

Malware

However, some attacks involve the use of malware; malicious software that is disguised as another type of file (such as documents, music tracks, images or videos), genuine software or apps in order to trick a user into opening, downloading or installing it onto their device. Some malware can even be installed onto a device simply by opening an infected website in a web browser.

Types of malware

https://swgfl.org.uk/security/types-of-malware/

Adware
A type of malware that tracks user activity (e.g. browser usage and downloads) with the intention of delivering advertising, which is often difficult to close.

Botnet
A botnet (from robot network) is a type of malware attack using multiple separate computers that have been infected and commanded by the attacker.

Keylogger
A keylogger can monitor a great deal of user activity, including email, browsing activity, program use and keystrokes, which can be used to acquire usernames and passwords.

Cryptocurrency miner
A miner (or 'cryptojacker') is designed to harness the computing power of the infected machine to generate cryptocurrency (e.g. Bitcoin) for the attacker.

Ransomware
A type of malware that infects the computer, but rather than causing damage, it encrypts data and demands payment (the 'ransom') in return for decrypting it.

Rootkit
A set of software tools designed to allow an attacker to gain unauthorised access - often elevated (e.g. administrator level) access - to a computer without being detected.

Spyware
A little like adware, spyware is a type of malware that monitors user activity and transmits this data to the attacker without the user's knowledge.

Trojan
Disguised as legitimate software, a trojan misleads the user in to executing it and allowing the payload to be deployed, which may include a 'backdoor' that an attacker can use to gain access.

Virus
A type of malware that attaches itself to legitimate programs or files, and replicates itself in order to 'infect' the computer and deploy the payload.

Worm
Unlike a virus, a worm can self-replicate without needing a host program or file, and often spreads without any user action, usually exploiting weaknesses (or 'vulnerabilities') in security measures.

Online privacy

https://www.youtube.com/watch?v=w2tW50CD6Aw&t=29s
This Barclays advert highlights how easy it can be for a criminal to build a data profile of a person based on things shared freely on social media or through other online content. This information can be used to guess passwords or even sign up for services or apply for credit in another person's name.

Limiting the availability of personal data to others online is therefore an important step for all online users to take, even young people. Although young people have limited access to financial services, a criminal could still use their details to apply for other online services.

These resources from the UK Safer Internet Centre and Internet Matters can help you manage privacy on popular social media apps and other online platforms.

Strong passwords
Strong and memorable passwords

The other best way to protect our data is to ensure that you use strong and memorable passwords on every online account and use a different password for each one.

Previous expert advice on passwords suggested that using upper- and lower-case letters, numbers and special characters would make passwords harder to guess or crack. While this is true, it also makes them very difficult to remember!

A better solution is to make a password based on three random words. There are a number of ways you can do this – you could use a random word generator, use a strategy like Diceware, or even make your own password dice to generate unique passwords, using the 'Making Strong Passphrases' activity on the School of Social Networks. These are also great strategies to share with students and colleagues!

Check this useful tool

https://howsecureismypassword.net/

Bibliography - " Digital Literacy and Online Safety" course , European SchoolNet