Cybersecurity Awareness and Training for schools

July 2025

Oide Technology in Education Website

https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/

Email: ictadvice@oide.ie

Overview

- What is Cybersecurity
- What is a Cyberattack

- HSE had a high profile 'Ransomware' attack on 14 May 2021
- Ransomware is just one type of cyberattack
- Other relevant risks: Phishing, Malware, Viruses, Spyware, Trojans

- Are schools systems and data at risk of a cyberattack?
- What type of cyber risks are relevant for schools?

- Some relevant resources, links etc.,

Data Brokers: Profiting from your data

- **Data brokers are companies that collect or purchase public, personal, private info' about you and then sell that data. (over 5,000 brokers, revenue of over €250 Billion per year)**
- **Consumer data is valuable, where you shop online, credit card details, coupons store's loyalty card, facebook pages you like, what you spend money on, birthday, addresses, your job title, your interests.**
- **Information on the Public Record: includes court records, motor vehicle records, census data, birth certificates, marriage licenses, voter registration information, bankruptcy records, divorce records.**
- **If you spend a lot of time on social media or in the online world, you're giving data brokers even more information about you. Data brokers collect personal info from the posts you've made or 'liked' online, online quizzes you've taken, and the websites you've visited.**
- **Some data brokers act legally using public data, many act illegally**

https://us.norton.com/blog/privacy/how-data-brokers-find-and-sell-your-personal-info

Ransomware attack on HSE (2021)

Took place on 14 May 2021

- All HSE systems were affected
- Forced to move to paper based system
- Confidential medical data was stolen, published online

- A malicious email was received on one PC on 16th March, it was opened 2 days later
- A Microsoft Excel attachment which contained 'malware' was downloaded
- 31st March: HSE AV software detected unusual activity, but checks were inconclusive
- Over next few weeks the attackers secretly gained further system access
- Attackers 'activated' ransomware on 14 May 2021, 8 weeks after the initial file attachment was download

Recovery:

- 6 weeks later, 75% of servers and 70% of devices were restored
- By Sept, 4 months later, 95% of servers & devices were restored
- Though no ransom was paid, the attack cost the HSE over €100 million

School data breach

Primary school pupils' data held to ransom by hackers

Data Protection Commissioner says school had lack of training on email attachments

https://www.irishtimes.com/news/ireland/irish-news/primary-school-pupils-data-held-to-ransom-by-hackers-1.3044951

- 2016: a data breach report from a primary school
- Ransomware attack by a third party.
- School's files, which included children's names, dates of birth and PPS numbers, inaccessible.

- The Commissioner found the school had deficiencies in the measures it had taken to secure pupils' personal data, including the fact that no polices or procedures were in place to maintain adequate back-ups.

- No procedures or policy documents focusing on system attacks such as ransomware or viruses and had no contracts in place with its ICT services providers, the data processors, as required by law.

- Actions by ICT suppliers were 'inadequate in response to the attack'.
- A lack of staff training and awareness of the risks associated with opening unknown email attachments or files.

- Commissioner found the school had broken the law by failing to ensure that adequate security measures were in place to protect the student data. Her office recommended to the school that it take steps 'to mitigate the risks identified'.

- The school implemented staff training on the risks associated with email and the use of personal USB keys and also reviewed its procedures to ensure appropriate contracts were in place with its ICT providers.

- Commissioner stated that: "This case demonstrates that schools, like other organisations interacting online must ensure that they have appropriate technical security and organisational measures in place to prevent loss of personal data, and to ensure that they can restore data in the event of crypto-ransomware attacks'

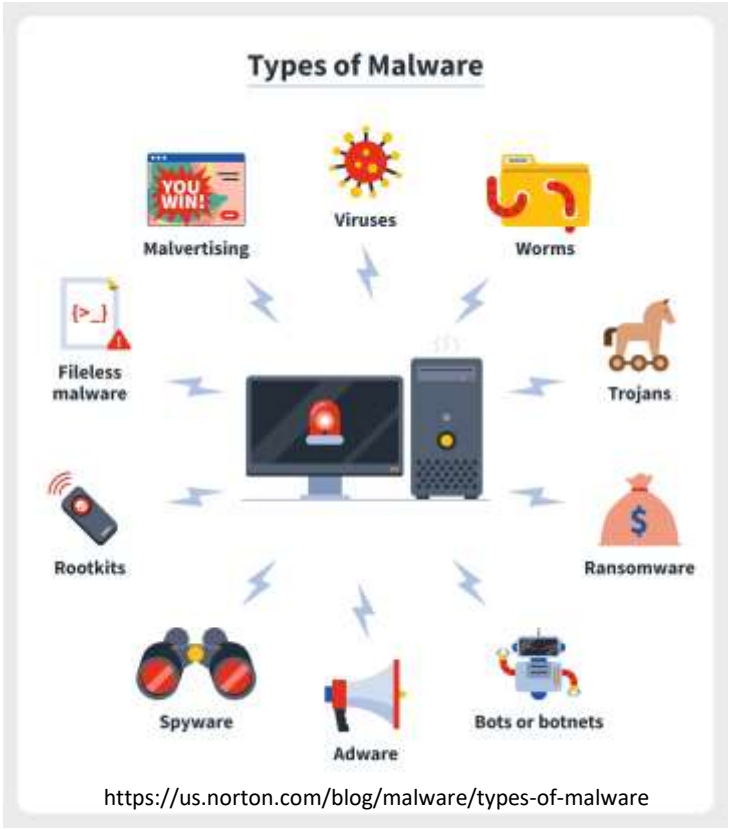
Schools and Cybersecurity

- If schools cannot or would not pay ransoms, why are they a target of cyberattacks?
- Schools have large numbers of potential targets, manage increasing amounts of personal data, and so this data can be seen as an 'attractive' target.
- Ransomware encrypts (ie. locks) all accessible or connected school devices
- May result in a full loss of digital data, including connected backups
- Mandatory reporting (GDPR) of a data breach to Office of Data Commissioner
- School 'Reputation', defacement of school website or social media accounts
- Significant workload and costs to restore systems and data – if possible
- In summary ramsomware attack will have a major negative impact on a school

Types of Cyberattack

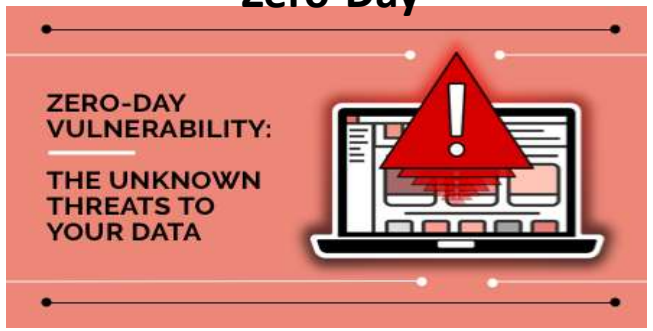
https://www.preemptive.com/five-evil-things-a-hacker-does-to-your-app/

https://www.avast.com/c-malware



https://us.norton.com/blog/malware/types-of-malware

Zero-Day



https://spanning.com/blog/zero-day-vulnerability/

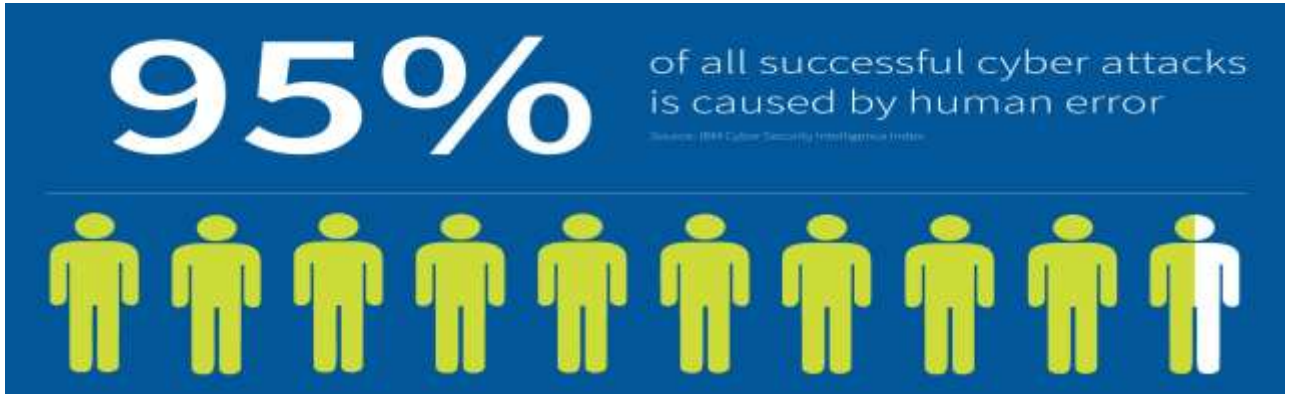
https://www.g2.com/articles/spoofing

Identity Theft

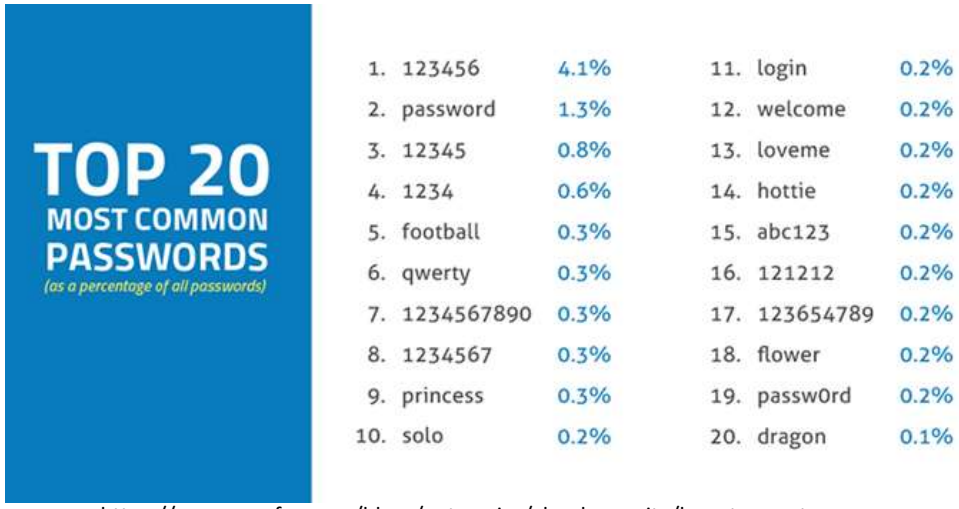
Ransomware

https://www.itprotoday.com/vulnerabilities-and-threats/how-tell-if-ransomware-message-real-or-fake

Human Factor, Internet of Things (IoT)



https://ssdtechie.com/2020/07/06/the-human-factor-in-cybersecurity-employees/

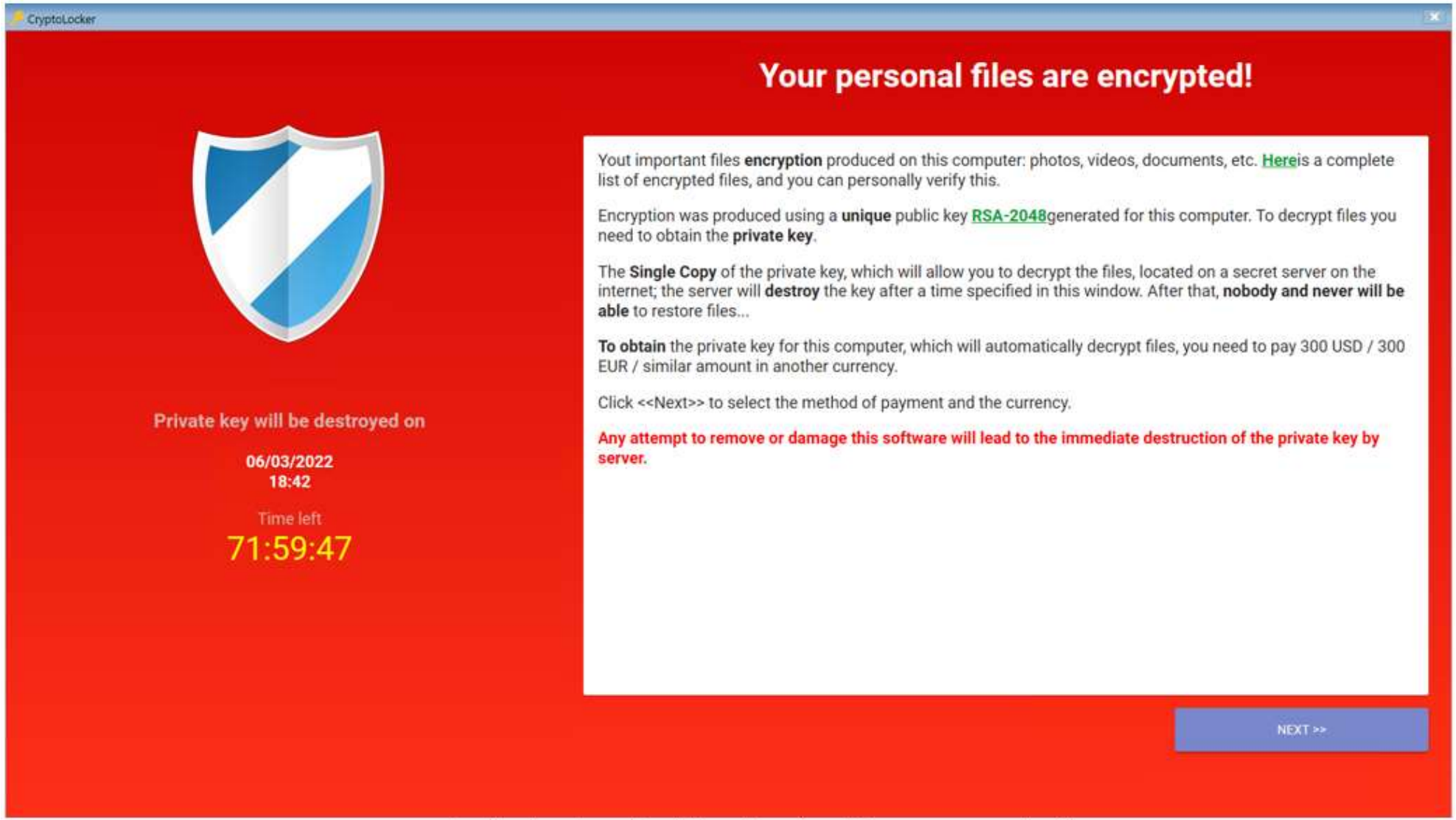


https://www.mcafee.com/blogs/enterprise/cloud-security/how-to-create-a-strong-password-you-actually-remember/

https://enterprisersproject.com/article/2016/2/internet-hackable-things-why-iot-devices-need-better-security

https://obtsynergy.com/why-you-are-your-biggest-online-security-threat/

Impact of Ransomware



https://www.itprotoday.com/vulnerabilities-and-threats/how-tell-if-ransomware-message-real-or-fake

Implications of Personal/Work mix

- Social media has a very strong presence in schools
- Risks in 'personal space' can become risks to the 'work/school space'
- Many users use the same passwords in Social Media and Work/Schools contexts
- This raises the cyber risk in schools
- Need to have different login details for personal/social and work accounts

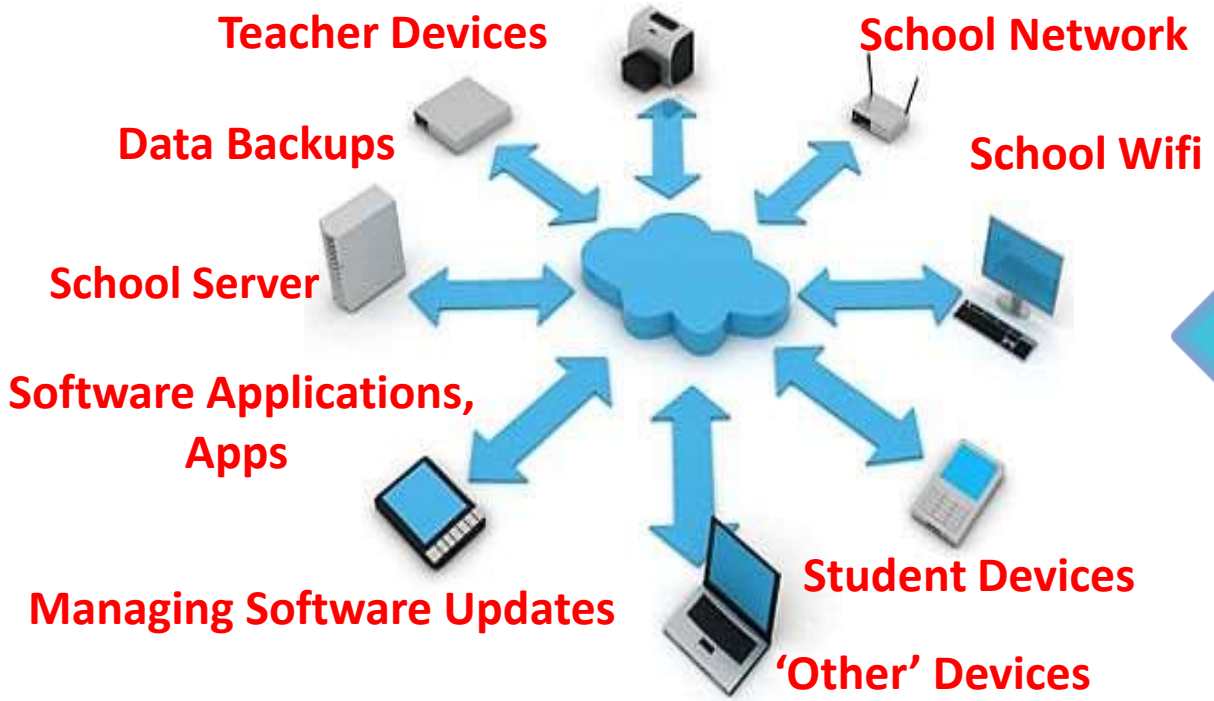
Personal

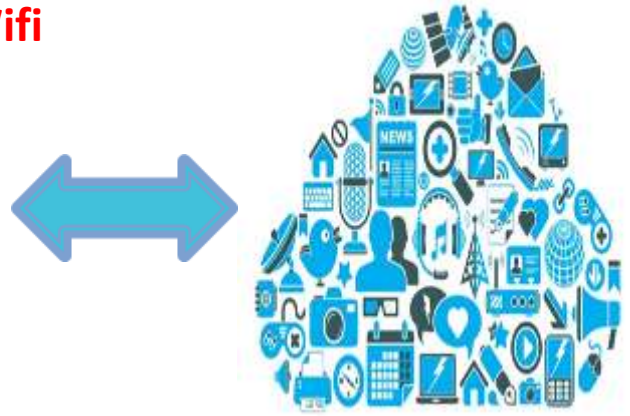
https://www.insurancebusinessmag.com/us/news/cyber/social-media-activity-exposing-many-users-to-cyber-risks--report-245417.aspx

Work/School

https://www.dnainfo.com/chicago/20170519/chinatown/st-therese-chinese-catholic-school-principal-phyllis-cavallone-jurek-stanley-c-golder-leadership-award/

Cyberattack Impact on Schools





Cloud based Services

- Payment systems
- Admin Systems
- Learning platforms
- Online Applications
- School Website
- Communications Systems with parents etc
- School App

External Parties

Prevention: Awareness/Education for Staff & Students

Improving Data and Cybersecurity

Who is targeting Schools

- **Online criminals:**
  Attempt to steal and sell important data using ransomware attacks etc.,

- **Hackers:**
  may not be financially motivated, but want to cause disruption or reputational damage to schools

- **Phishing Campaigns:**
  These attacks leverage 'social engineering' and mimic genuine providers to deceive schools into providing login and password details, credit card information etc.,

- **Malicious Insiders:**
  Disgruntled staff or unhappy students may use their access to a school's IT systems to carry out malicious activity to cause disruption or reputational damage.

- **'Indiscriminate or Untargeted' cyberattacks:**
  don't care who the victim is, they target as many users as possible. They use techniques such as 'phishing', 'water-holing' and 'port scanning'

Guide: Cyber Security for schools:
https://ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Schools.pdf

Some Cybersecurity Terms

Glossary

- **Credentials - A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.**
- **Decryption – taking encoded or encrypted text or other data and converting it back into text you or the computer can read and understand**
- **Encryption - A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.**
- **Firewall - Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to or from a network.**
- **Multi-factor authentication - The use of two different components to verify a user's claimed identity.**
  Patching - Applying updates to firmware or software to improve security and/or enhance functionality.
  Phishing - Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
- **Port scanning - A port scan is a common technique hackers use to discover open doors or weak points in a network.**
- **Ransomware - Malicious software that makes data or systems unusable until the victim makes a payment.**
- **Water-holing - Setting up a fake website (or compromising a real one) in order to exploit visiting user**
- **Many more …**

Viruses – Need for AV on different types of devices

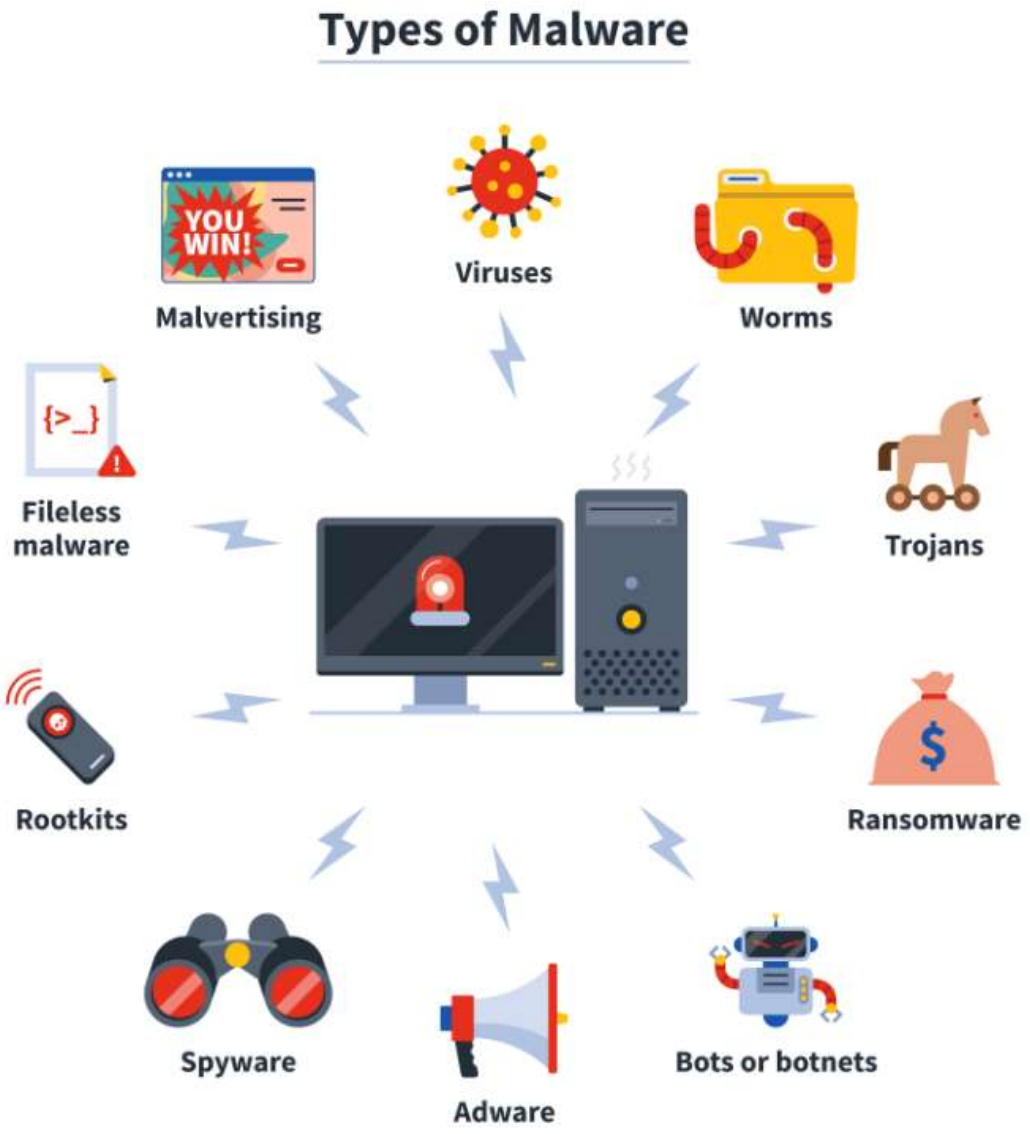
- A software virus is a type of malicious software, or malware, that attaches itself to existing files, for example to Microsoft Excel or Word files.
- When these files are opened the virus activates and spreads between computers and causes damage to data and software.
- Viruses aim to disrupt systems, cause operational issues, and result in data loss and leakage.
- Virus can be used with other types of malware to carry out ransomware attacks.
- Viruses need a user action, such as opening a file, to activate.
- Other types of malware such as worms don't need a user action to be activate.

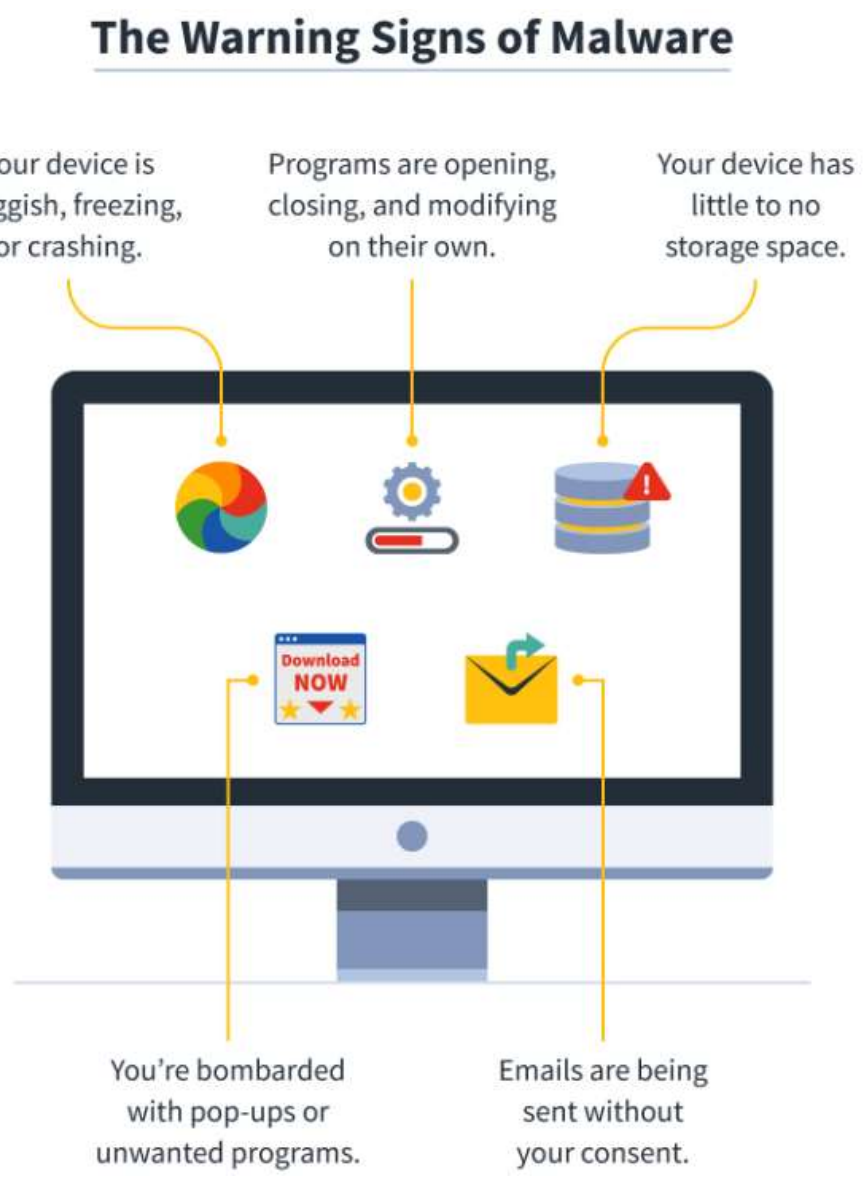
- Antivirus (AV) is software that detects, and quarantines the virus. Using a regularly updated database of malware and viruses, it scans a device for viruses. No antivirus protection is 100% effective but is recommended especially for Windows based devices.

- Chromebooks and Apple devices may be considered a 'lower risk' of being infected by 'viruses', however they are still at risk from other cyberattacks including phishing etc.

https://www.security.org/antivirus/

Impact of Malware

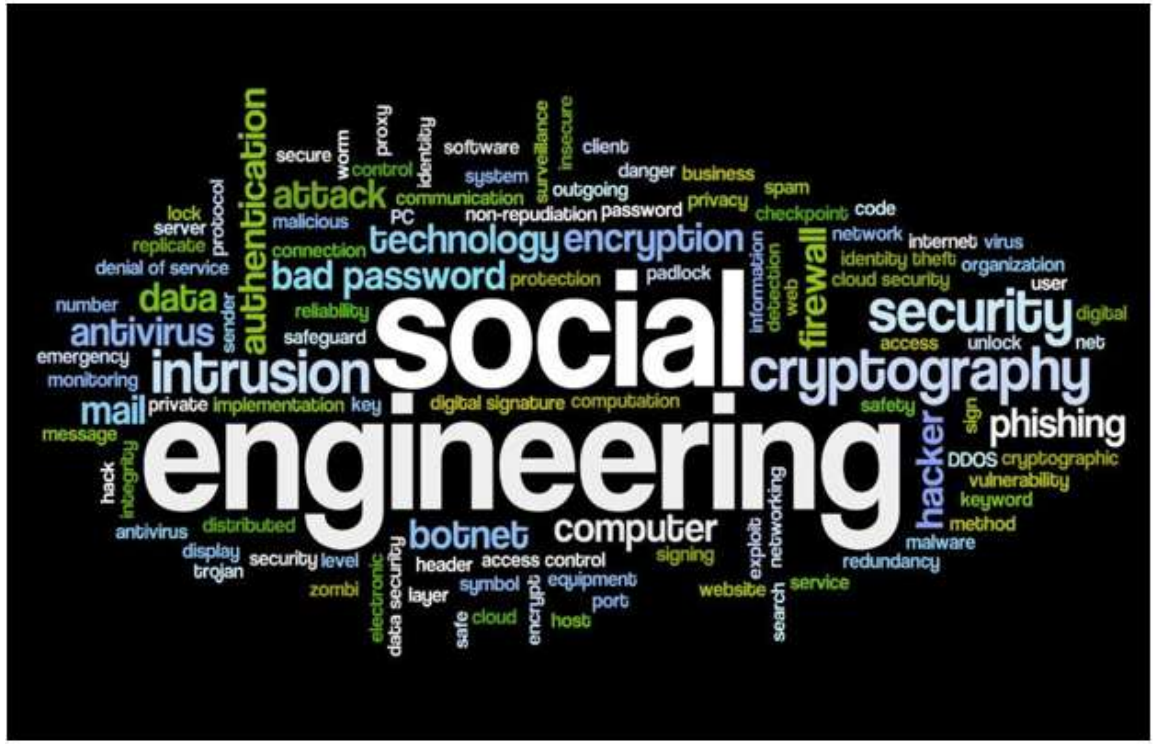




https://us.norton.com/blog/malware/types-of-malware

Social Engineering

- Many cyberattacks use techniques known as social engineering
- This is based on human psychology and understanding how we 'humans' think and act
- What motivates our actions
- It exploits how we can be manipulated into unknowingly taking actions that may result in providing 'access' to data
- Attacks can happen online, via email, or in direct communication with external parties
- High priority alerts are used to cause user anxiety/panic
- This can cause users to act un-intentionally (eg., alerts of problems with bank accounts, tax, overdue payment, loss of critical service)



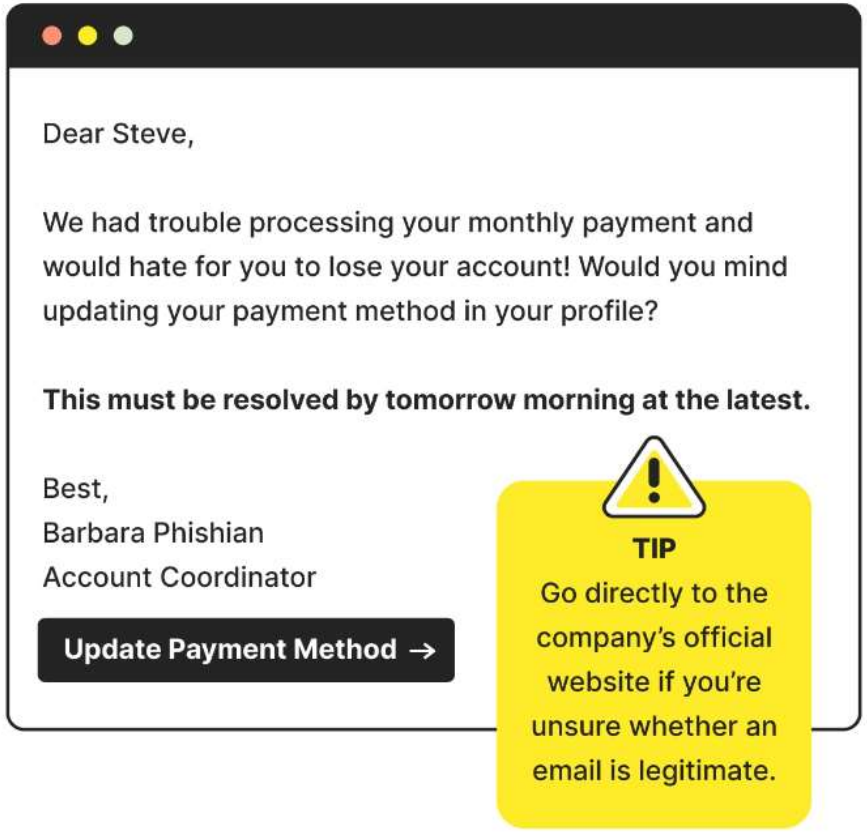
https://threatpost.com/rethinking-responsibilities-social-engineering-attacks/148466/

What is Phishing?

- **Social engineering is the 'art' of exploiting human psychology. Today's cyber attackers are combining social engineering and technology for profit.**
- **According to the InfoSec Institute, phishing is the most commonly used social engineering attack.**
- **These attacks leverage social engineering to trick victims into giving up sensitive information such as passwords or credit card information.**

https://www.csoonline.com/article/2117843/what-is-phishing-examples-types-and-techniques.html

https://us.norton.com/blog/privacy/5-tips-for-social-media-security-and-privacy

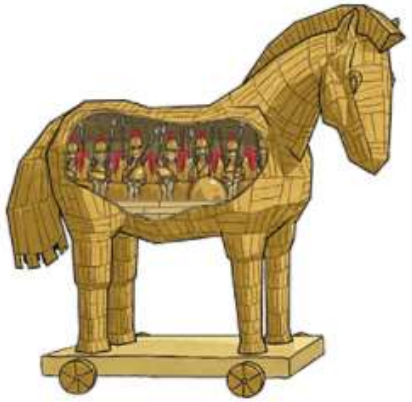


Malware attacks

- Malware: (Malicious software)
- Any program or file that's harmful to computers or data

https://www.packetlabs.net/posts/pipedream-malware-toolkit/

- Includes viruses, spyware, keyloggers, ransomware & trojans
- Virus: malware that makes copies of itself and inserts these into other files
- Spyware: malicious software designed to gather data, and send it to 3rd parties
- Keyloggers: records keystrokes, recording everything you type on a keyboard
- Ransomware (already discussed)



- Trojans: malware that conceals its real content. Like the 'Trojan Horse' used to attack the city of Troy (~1200 BC), harmful content is hidden 'within' the trojan delivery agent

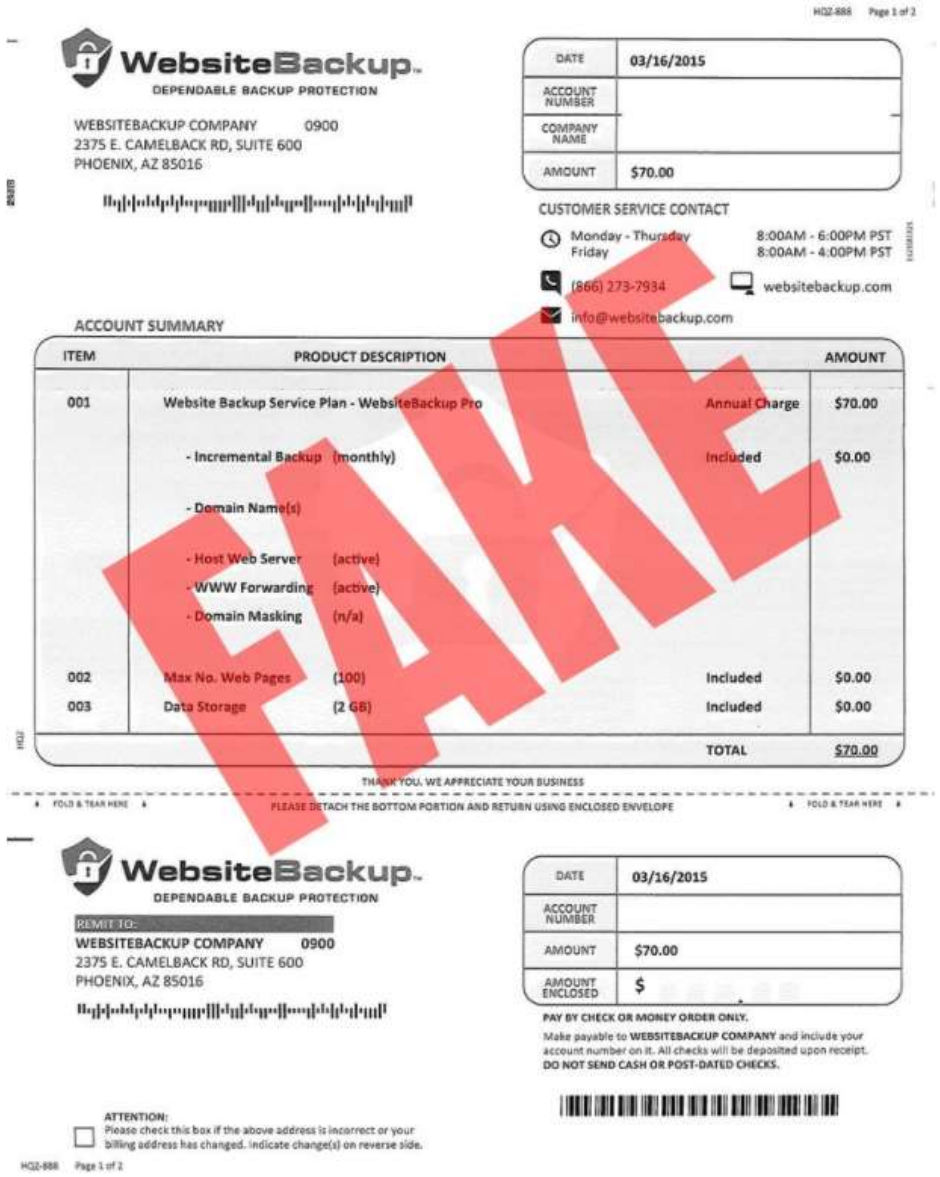
Phishing Attack

- Phishing is not a type of ‘Malware’
- It’s a method of attack to access private information, using social engineering / deception
- Tries to deceive users into unknowingly divulging confidential information
- Phishing can occur through email ‘spoofing’ or phone calls where an attacker pretends to be a ‘trusted’ party

https://business-review.eu/tech/online/what-is-a-phishing-attack-and-how-do-you-steer-clear-of-them-224941

- Often phishing attacks are indiscriminately directed towards a large number of users by email or phone
- When hackers specifically target an individual user, this is known as ‘spear phishing’

Phishing Invoice attack



WebsiteBackup
DEPENDABLE BACKUP PROTECTION

WEBSITEBACKUP COMPANY 0900
2375 E. CAMELBACK RD, SUITE 600
PHOENIX, AZ 85016

DATE	03/16/2015
ACCOUNT NUMBER	
COMPANY NAME	
AMOUNT	$70.00

CUSTOMER SERVICE CONTACT
Monday - Thursday 8:00AM - 6:00PM PST
Friday 8:00AM - 4:00PM PST
(866) 273-7934 websitebackup.com
info@websitebackup.com

ACCOUNT SUMMARY

ITEM	PRODUCT DESCRIPTION		AMOUNT
001	Website Backup Service Plan - WebsiteBackup Pro	Annual Charge	$70.00
	- Incremental Backup (monthly)	Included	$0.00
	- Domain Name(s)		
	- Host Web Server (active)		
	- WWW Forwarding (active)		
	- Domain Masking (n/a)		
002	Max No. Web Pages (100)	Included	$0.00
003	Data Storage (2 GB)	Included	$0.00
		TOTAL	$70.00

FAKE

THANK YOU. WE APPRECIATE YOUR BUSINESS

FOLD & TEAR HERE — PLEASE DETACH THE BOTTOM PORTION AND RETURN USING ENCLOSED ENVELOPE — FOLD & TEAR HERE

WebsiteBackup
DEPENDABLE BACKUP PROTECTION

REMIT TO:
WEBSITEBACKUP COMPANY 0900
2375 E. CAMELBACK RD, SUITE 600
PHOENIX, AZ 85016

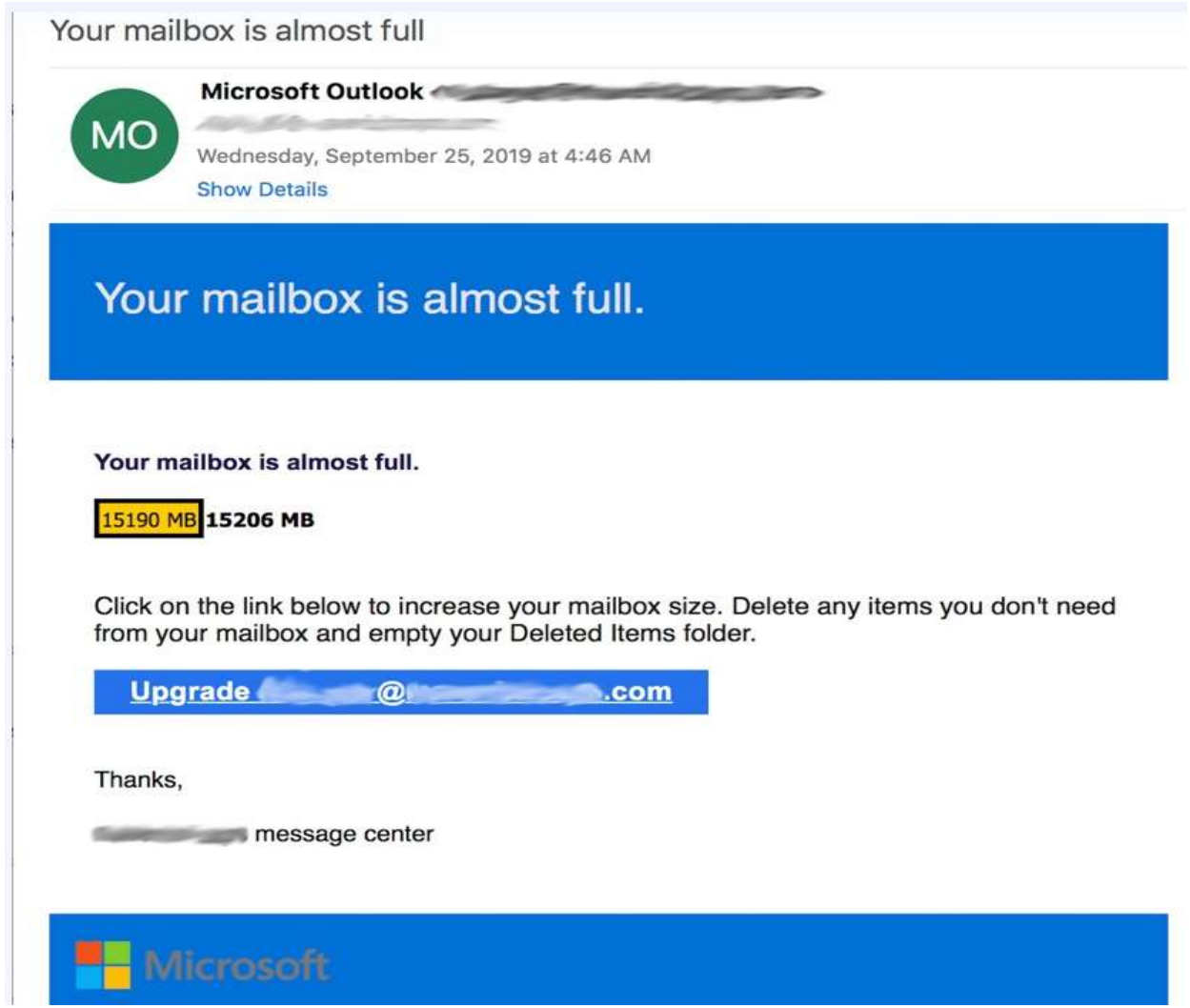
DATE	03/16/2015
ACCOUNT NUMBER	
AMOUNT	$70.00
AMOUNT ENCLOSED	$

PAY BY CHECK OR MONEY ORDER ONLY.
Make payable to WEBSITEBACKUP COMPANY and include your account number on it. All checks will be deposited upon receipt.
DO NOT SEND CASH OR POST-DATED CHECKS.

ATTENTION:
Please check this box if the above address is incorrect or your billing address has changed. Indicate change(s) on reverse side.

- **Phishing - method of accessing data using social engineering / deception**
- **Email with attached Invoice from a 3rd party attacker**
- **Invoice is designed to look like the legitimate company that the school uses for website services**
- **Raises anxiety that if invoice is not paid the service may be affected**

Phishing email from software provider


Your mailbox is almost full

MO

Microsoft Outlook [redacted]

[redacted]

Wednesday, September 25, 2019 at 4:46 AM

Show Details

Your mailbox is almost full.

Your mailbox is almost full.

15190 MB 15206 MB

Click on the link below to increase your mailbox size. Delete any items you don't need from your mailbox and empty your Deleted Items folder.

Upgrade [redacted]@[redacted].com

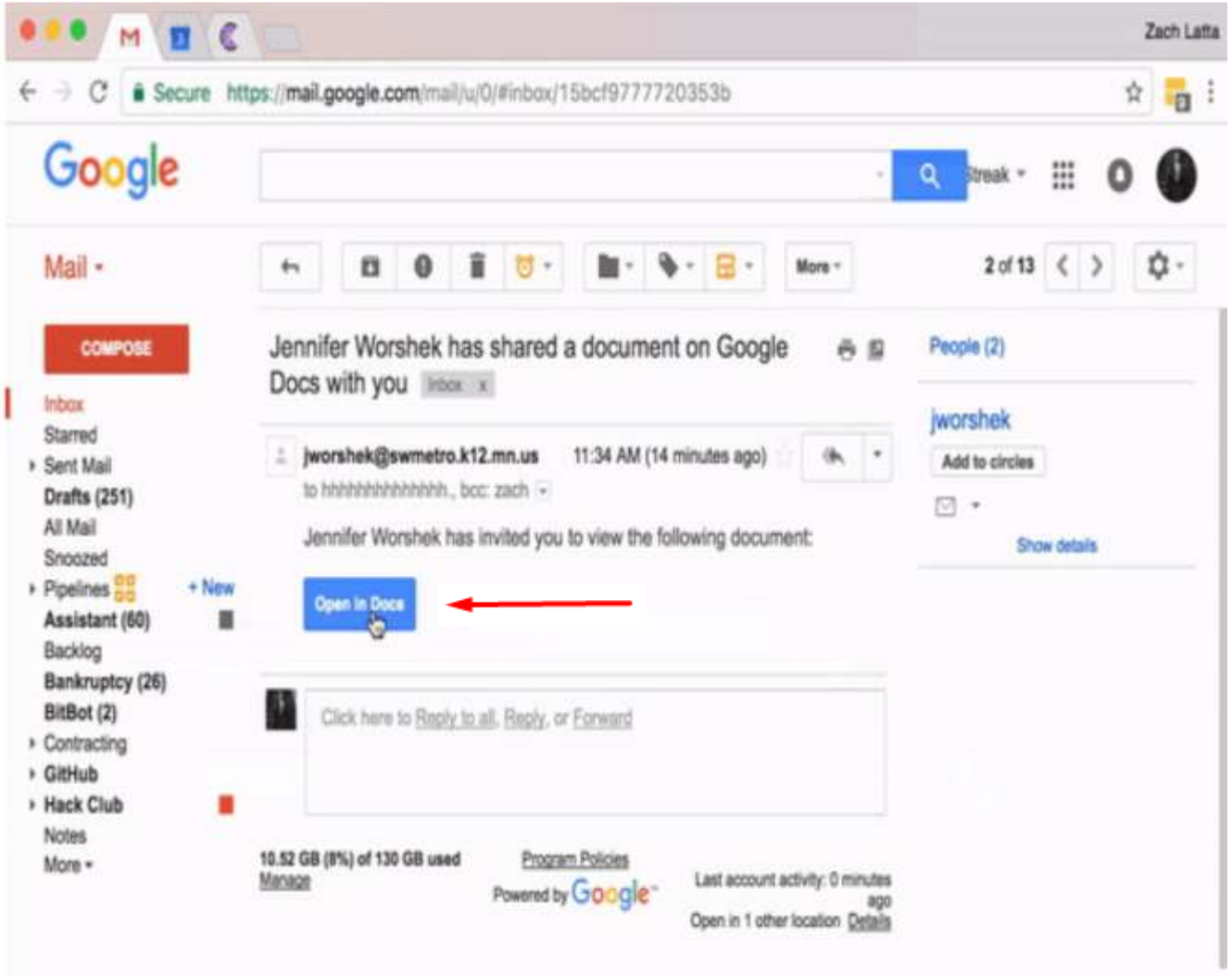
Thanks,

[redacted] message center

Microsoft

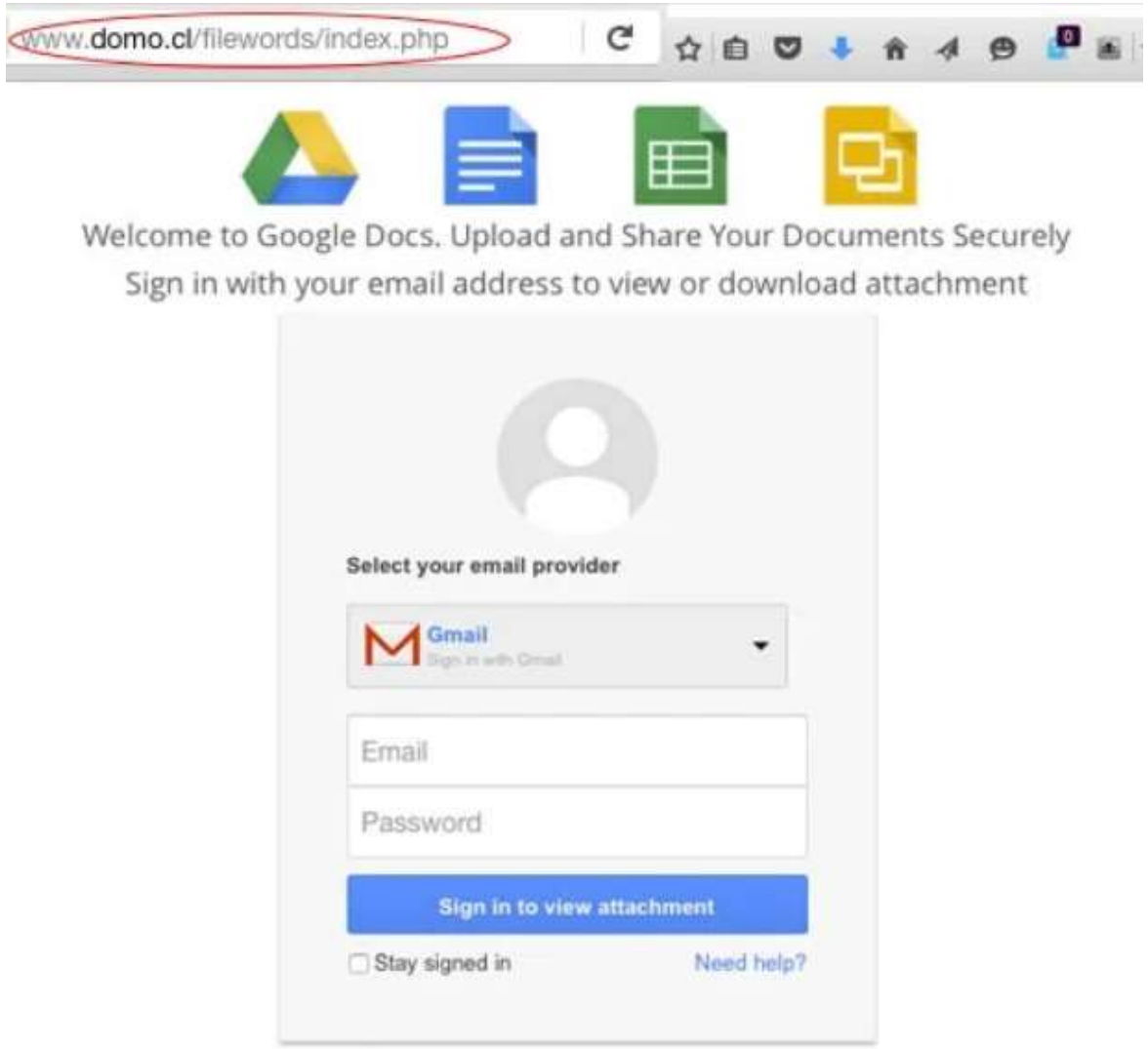
- Phishing email with request to take immediate action
- Tries to impersonate a legitimate company that the school uses for online services
- Raises anxiety that if action is not taken the service could stop working

Phishing invite in Google Docs



- This phishing request **invites** the user to **click on a malicious link**
- **Designed to look like a familiar process** that schools use on a regular basis
- This could **target staff or students** within a school

Phishing - Domain Spoofing



- This phishing request invites a user to login to a malicious website
- Designed to look like a trusted website that schools already use
- Could target staff or students within a school

New Email – Open or Delete?

CAUTION: This email originated from an external source. Do not click links or open attachments unless the sender is known.

Danger Signs:- <u>Delete emails without opening them if:</u>

- You don't recognize the sender
- It's a generic/mass/bulk email
- It's not addressed to a specific person
- It looks 'unusual'
- Something doesn't feel right about it
- It requests an urgent response
- You feel under pressure to act
- It's unexpected
- Special offer, OIALO, TGTBT
- An 'appeal' for financial support
- Requests that you *'click on a link'*
- It's refers to an problem with your bank account, credit card, package delivery/unpaid fee, software renewal, service expiry, your password etc.,

- Unless you know and trust the sender don't click on attachments

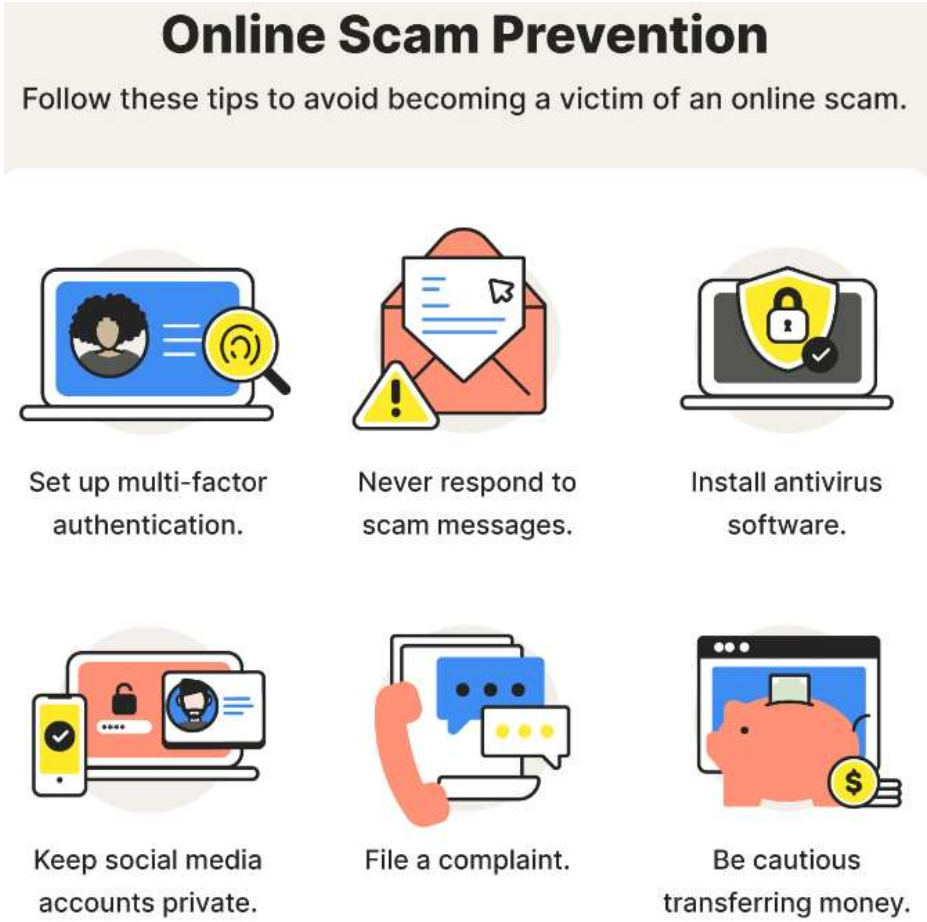
https://www.komando.com/tech-tips/migrate-email-between-accounts/707359/

Beware of Scams

Scams: using internet services or software to defraud or take advantage of victims, typically for financial gain.

Online scams: Top 20 internet scams

- Phishing scams
- Ransomware
- Scareware
- Travel scams
- Fake shopping websites
- Grandparent scams
- Romance scams
- Hitman scams
- Lottery scams
- Tech support scams
- Disaster relief scams
- COVID-19 scams
- The Nigerian letter scams
- Money transfer scams
- Pre-approved notice scams
- Cryptocurrency scams
- Social media scams
- Social media impersonation
- Mobile scams
- Job offer scams



https://us.norton.com/blog/emerging-threats/internet-scams

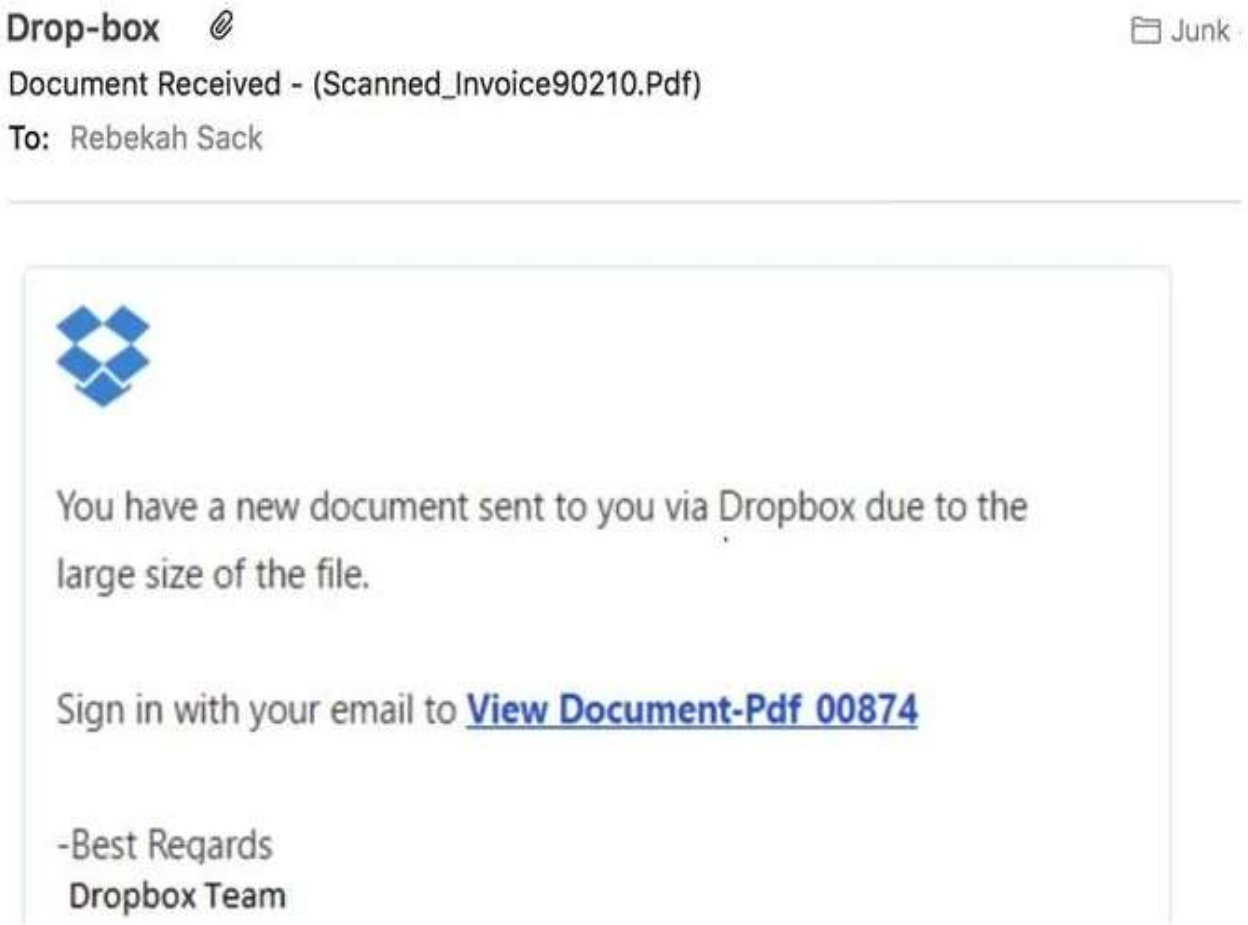
Privacy: Social Media Cleanup

Social Media Cleanup Checklist: A 9-step cybersecurity guide

- [x] Find all of your social media accounts
- [x] Make your accounts private
- [x] Delete any inappropriate posts or comments
- [x] Deactivate any unused accounts
- [ ] Clean up your followers and friends list
- [ ] Unfollow any inappropriate accounts
- [ ] Use appropriate profile pictures
- [ ] Think about your personal data
- [ ] Routinely update your passwords

https://us.norton.com/blog/privacy/social-media-clean-up

Phishing email from Cloud Provider



- This phishing email invites the user to click on a link to malware
- Looks like a familiar service that schools already use
- This could target any staff or students in a school

Spotting Fake/Spoofing Websites

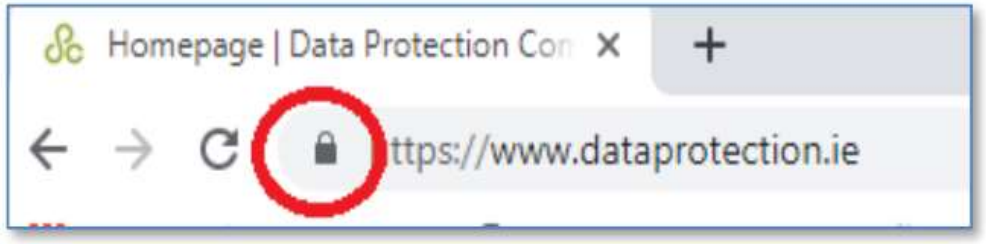
- **Examples of 'Trusted' Websites**
  - **Dataprotection.ie**
  - **Education.ie**
  - **Scoilnet.ie**
  - **pdsttechnologyineducation.ie**

- **Trusted sites are secure (use encryption) to prevent eavesdropping on data**

- **The have a 'padlock' symbol**

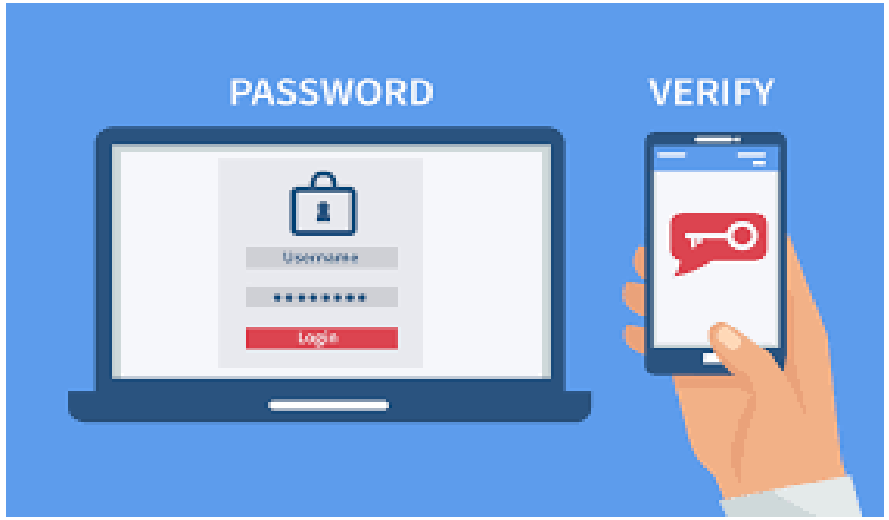
- **"https" ('s' indicated secure) rather than just "http" or 'www'.**

https://www.pandasecurity.com/en/mediacenter/security/what-makes-websites-trustworthy/



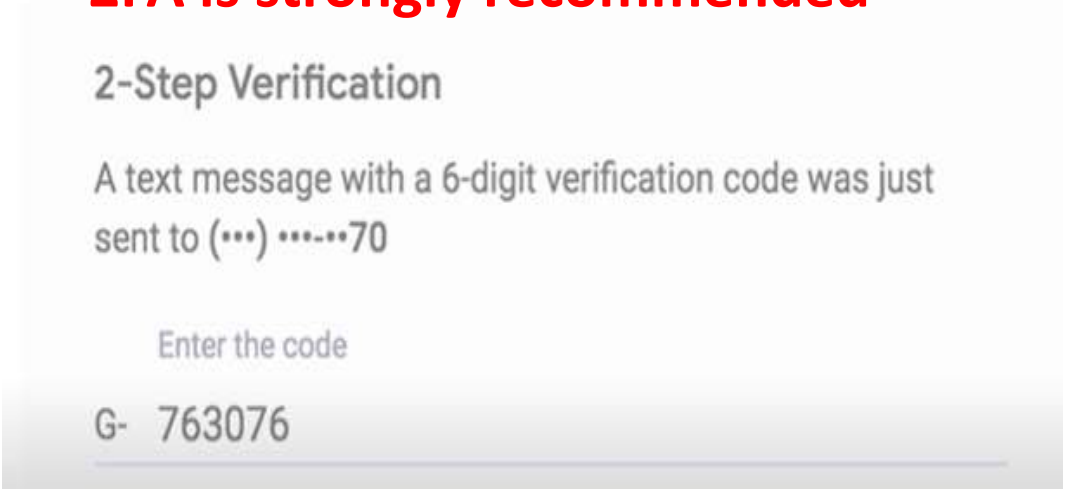
Managing Passwords

- **Managing passwords is critical to cybersecurity.** Affects all computer based or online activities.
- **No personal or social media passwords to be used on school devices**
- Good password management can take significant effort, but **not doing so exposes users to SERIOUS RISK!**
- **Your activity may impact you school, and can be traced back to particular devices** (as per HSE attack one 1 PC)
- Two Factor Authentication (2FA) uses **two separate ways to login**, eg., 1: email/password, 2: code received by text message



https://www.malwarebytes.com/blog/news/2018/09/two-factor-authentication-2fa-secure-seems

2FA is strongly recommended



Passwords – Some Tips

- Never reveal your passwords to others
- Use different passwords for different accounts. Never use the same passwords for work/personal use
- Use Two-Factor Authentication (2FA)
- Use long passwords: Min 8 characters long, ideally 12 characters
- Use ‘hard to guess’ but ‘easy to remember’
- Don’t use single dictionary words, date of birth, favourite teams, child or pet names, these can be easily found on social media
- Use ‘complexity’: eg., include upper and lower case letters, numbers, and special characters

https://www.iteksolutions.ca/strong-passwords-the-importance-in-the-workplace-and-how-to-create-one/

- Consider using a Password Manager
- Many advantages, however firstly understand how they work:

Some examples of Password Managers

- RoboForm
- Keeper
- 1Password
- NordPass
- Total Password

Guidance on Cybersecurity: Useful Links

The National Cyber Security Centre
https://ncsc.gov.ie/guidance/

Quick Guide: Cyber Security for schools:
https://ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Schools.pdf

Guidance on ransomware
https://www.ncsc.gov.ie/ransomware/

Citizensinformation.ie
https://www.citizensinformation.ie/en/consumer/buying-digital-content-and-services/scams-and-fraud/

Some other relevant website links:
https://www.garda.ie/en/crime/fraud/

https://www.fraudsmart.ie/personal/fraud-scams/

https://www.fraudsmart.ie/personal/fraud-scams/email-fraud/phishing/

Oide Technology in Education – Cybersecurity Guidance and Supports

Thank You

Please send any queries to ictadvice@oide.ie