

Cybersecurity Risks & Implications for schools

**ETBI Annual Conference
Sligo**

25th January 2023



Tom Lonergan

PDST Technology in Education

<https://www.pdsttechnologyineducation.ie/technology-infrastructure/>

Email: ictadvice@pdst.ie

pdst Technology in Education

+ Courses & Practice

+ Projects & Initiatives

+ Digital Technology Infrastructure

+ Contact

OUR ROLE IS TO

promote and support the integration of technology in teaching and learning

VIEW ALL NEWS ▶

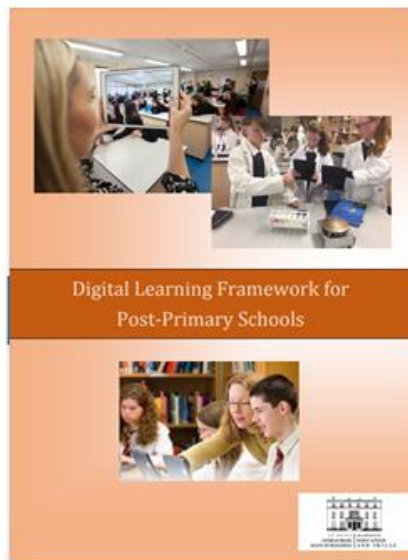
Courses & Practice

Projects & Initiatives

Digital Technology Infrastructure



Digital Strategy for
Schools to 2027



Digital Learning
Framework for
Schools



Digital Learning
Planning Guidelines



Digital Learning
Plan

- **Profit is the driver for cyberattacks**
- **Data brokers are companies that collect or purchase public, personal, private info' and then sell that data. (~5,000 brokers, revenue of €250 Billion/year)**
- **Consumer data is valuable, where you shop online, credit card details, coupons store's loyalty card, social media activity, what you spend money on, birthdays, addresses, your interests.**
- **Information on the Public Record:** includes court records, motor vehicle records, census data, birth cert, marriage licenses, voter registration etc.,
- **Social media users readily give their data to these brokers, who** collect personal info from the posts made or 'liked', online quizzes you've taken, and websites you've visited.
- **Some data brokers act legally using public data, many act illegally**



<https://www.youtube.com/watch?v=uZ2l-kk5ihk>

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

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 initial file 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 €150 million**

Primary school pupils' data held to ransom by hackers

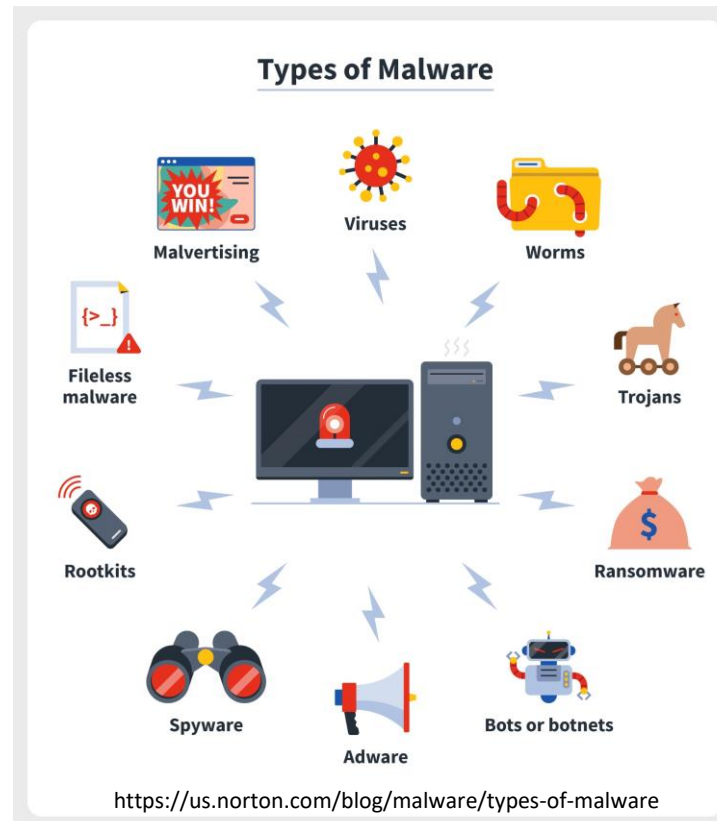
Data Protection Commissioner says school had lack of training on email attachments

<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.
- Data Commissioner found the school had **deficiencies in the measures it had taken to secure pupils' personal data**, including the fact that **no policies or procedures** were in place to maintain adequate back-ups.
- 'No procedures on system attacks and 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 student data. Recommended that **school take steps 'to mitigate the risks identified'**.
- **School implemented staff training**, and 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** 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**'



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



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

<p>RANSOMWARE</p> <p>Blackmails you</p>	<p>SPYWARE</p> <p>Steals your data</p>	<p>ADWARE</p> <p>Spams you with ads</p>
--	---	--

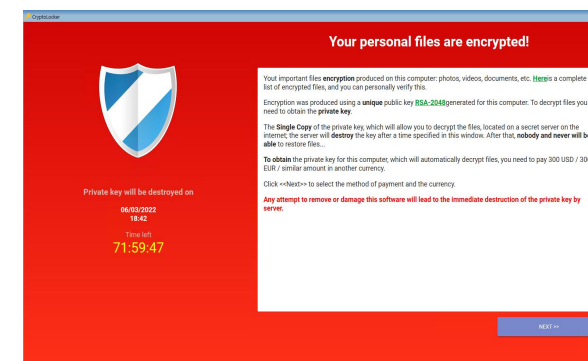
Types of Malware

<p>WORMS</p> <p>Spread across computers</p>	<p>TROJANS</p> <p>Sneak malware onto your PC</p>	<p>BOTNETS</p> <p>Turn your PC into a zombie</p>
--	---	---

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

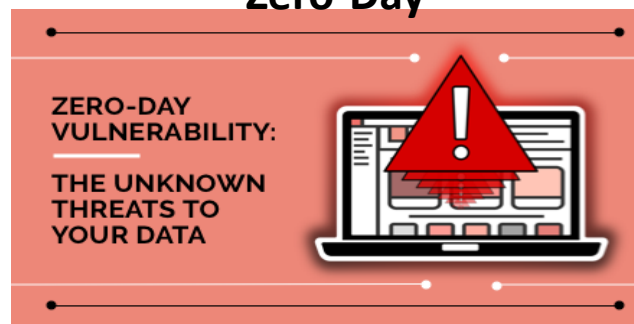
Identity Theft

Ransomware



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

Zero-Day



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



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

TOP 20 MOST COMMON PASSWORDS

(as a percentage of all passwords)

1. 123456	4.1%	11. login	0.2%
2. password	1.3%	12. welcome	0.2%
3. 12345	0.8%	13. loveme	0.2%
4. 1234	0.6%	14. hottie	0.2%
5. football	0.3%	15. abc123	0.2%
6. qwerty	0.3%	16. 121212	0.2%
7. 1234567890	0.3%	17. 123654789	0.2%
8. 1234567	0.3%	18. flower	0.2%
9. princess	0.3%	19. passw0rd	0.2%
10. solo	0.2%	20. dragon	0.1%

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

COMMON IoT DEVICES

That Could Get Compromised




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



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

CryptoLocker

Your personal files are encrypted!



Private key will be destroyed on
06/03/2022
18:42
Time left
71:59:47

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt files you need to obtain the **private key**.

The **Single Copy** of the private key, which will allow you to decrypt the files, located on a secret server on the internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

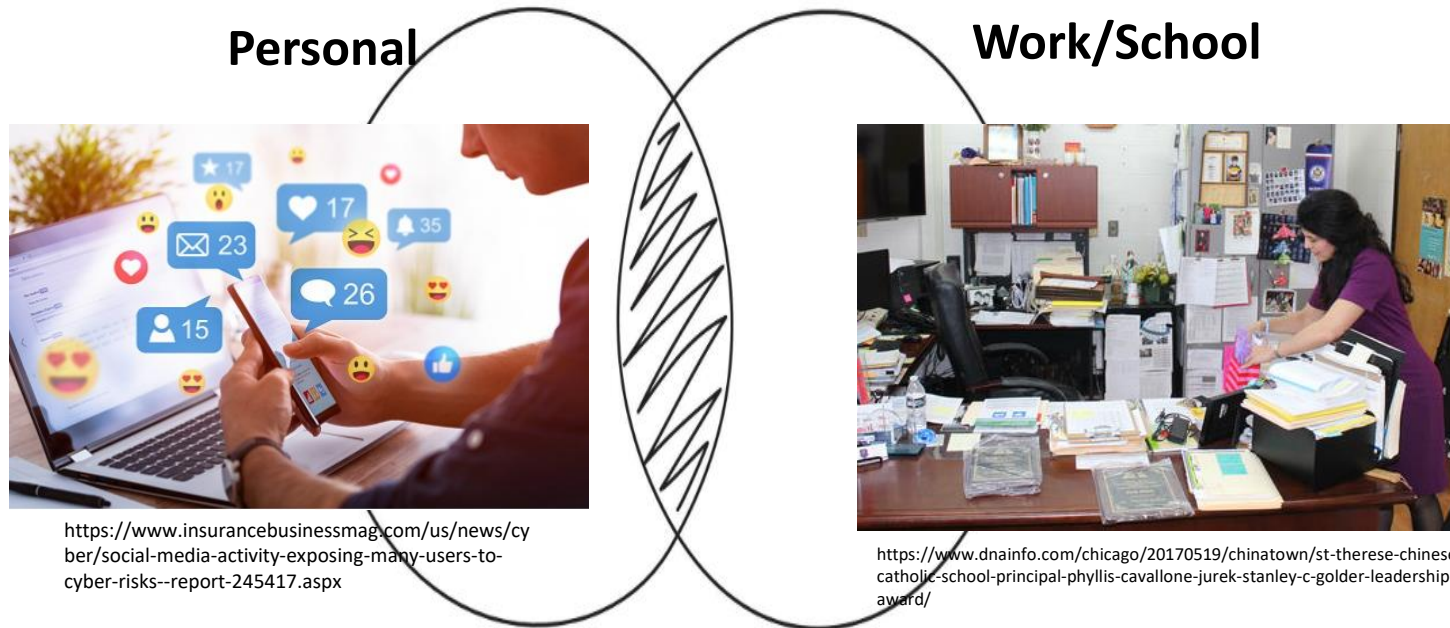
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click <<Next>> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

NEXT >>

- **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.



- Some may think that as schools cannot or would not pay ransoms, **they may not be a target of cyberattacks?. This is not the case.**
- 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**
 - **A Cyberattack could close your school**



- **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.



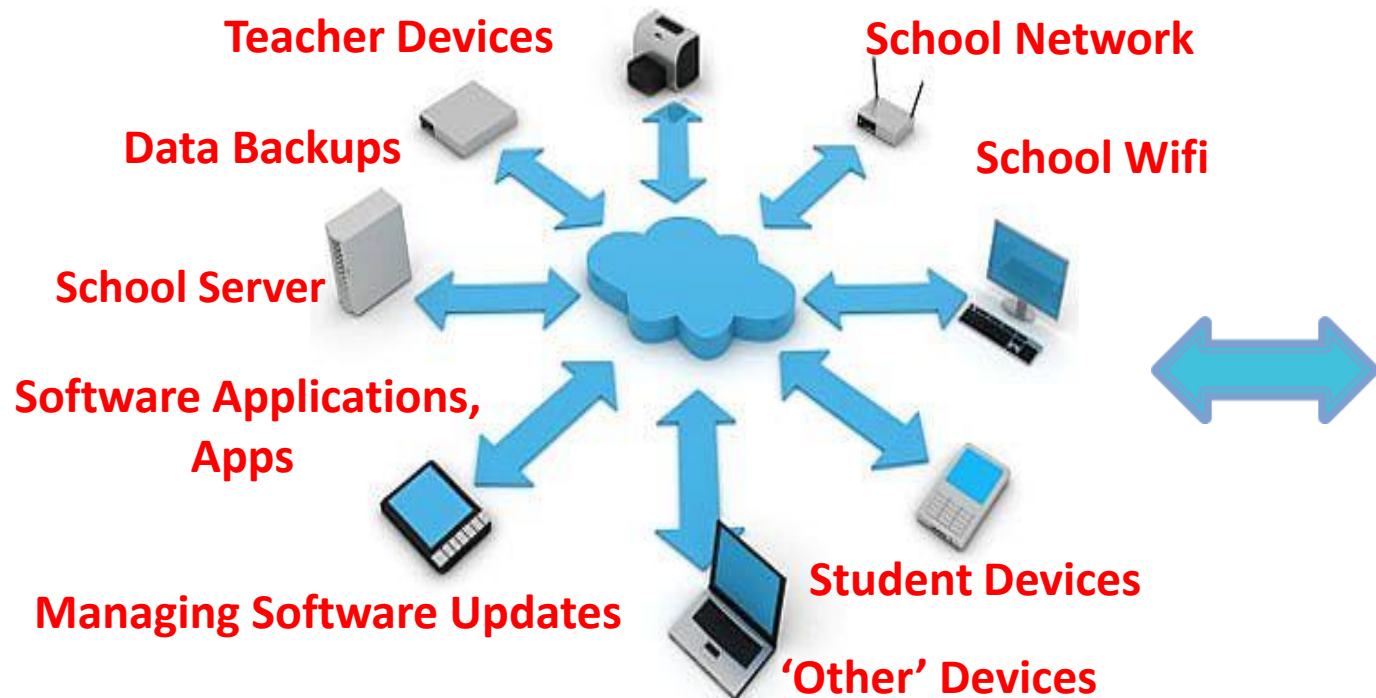
- **‘Indiscriminate or Untargeted’ cyberattacks:**
don’t care who the victim is, they target as many users as possible. They use techniques such as ‘phishing’, ‘water-holing’ and ‘port scanning’

Guide: Cyber Security for schools:

https://ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Schools.pdf

Glossary

- **Credentials** - A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.
- **Encryption** - A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.
- **Decryption** – taking encoded or encrypted text or other data and converting it back into text you or the computer can read and understand
- **Firewall** - Hardware or software which uses defined rules to constrain network traffic to prevent unauthorised network access.
- **Multi-factor authentication** - The use of two different components to verify a user's claimed identity
- **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 common technique hackers use to discover 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 ...



Cloud based Services

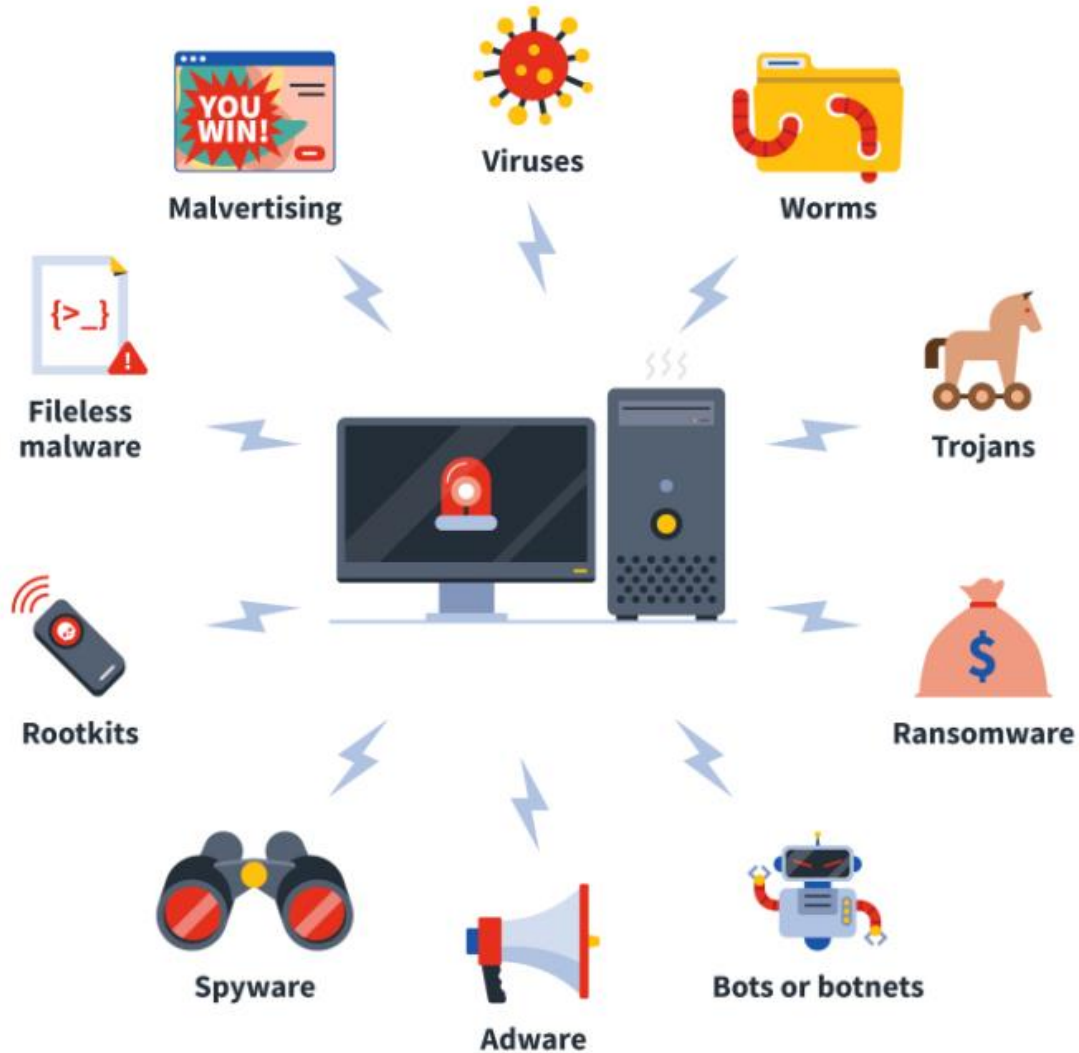
- Payment systems
- Admin Systems
- Learning platforms
- Online Applications
- School Website
- Communications with parents
- School App

External Parties

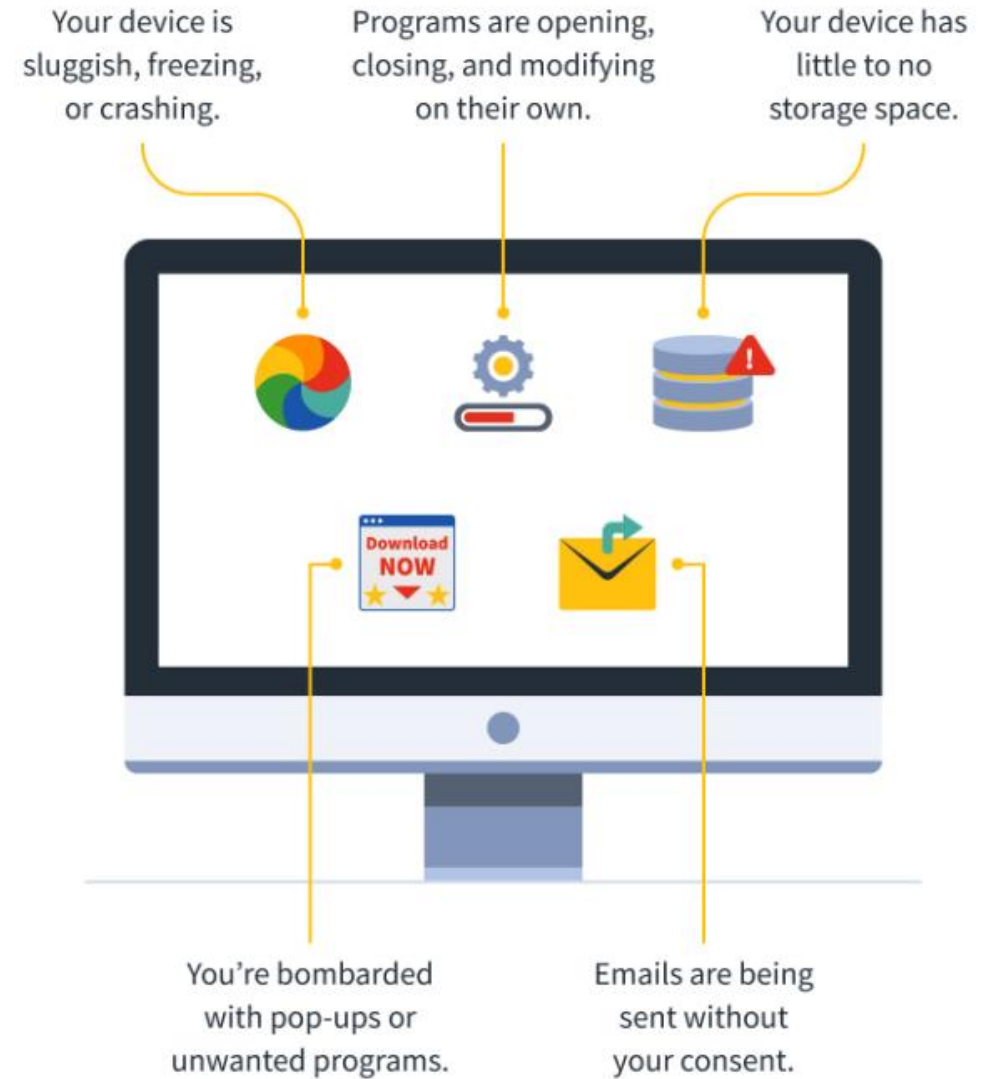
**Prevention: Awareness/Education
for Staff & Students**

**Improving Data and
Cybersecurity**

Types of Malware



The Warning Signs of Malware



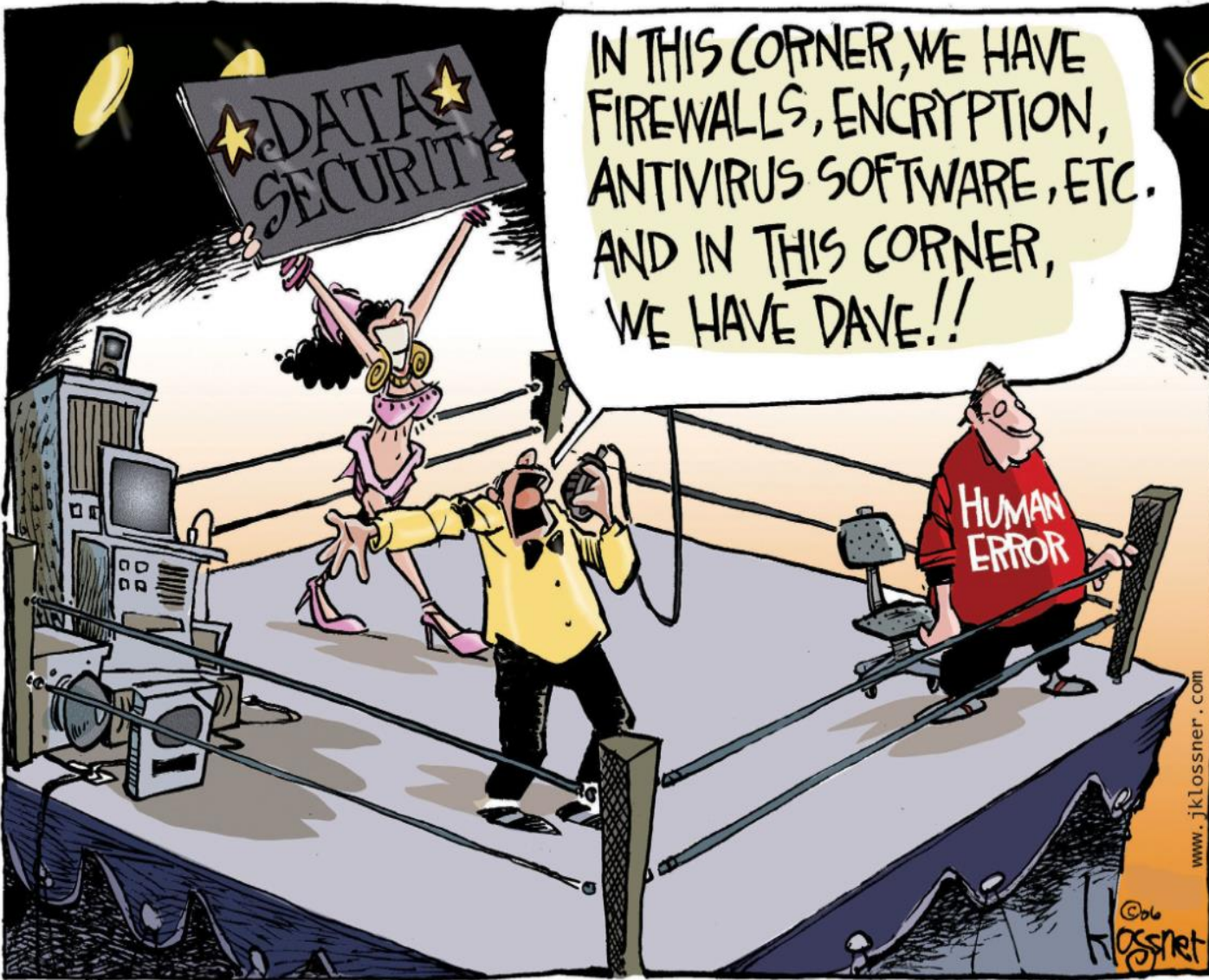
- **Social engineering** is the ‘art’ of exploiting human psychology. Today’s cyber attackers are combining social engineering and technology for profit.
- According to the [InfoSec Institute](#), **phishing** is the most common type of social engineering attack.
- These attacks trick victims into giving 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>



A screenshot of a web browser window displaying a phishing email. The email text reads: 'Dear Steve, We had trouble processing your monthly payment and would hate for you to lose your account! Would you mind updating your payment method in your profile? This must be resolved by tomorrow morning at the latest. Best, Barbara Phishian Account Coordinator'. Below the text is a dark button that says 'Update Payment Method →'. To the right of the email content is a yellow callout box with a warning icon (a triangle with an exclamation mark) and the text: 'TIP Go directly to the company's official website if you're unsure whether an email is legitimate.'

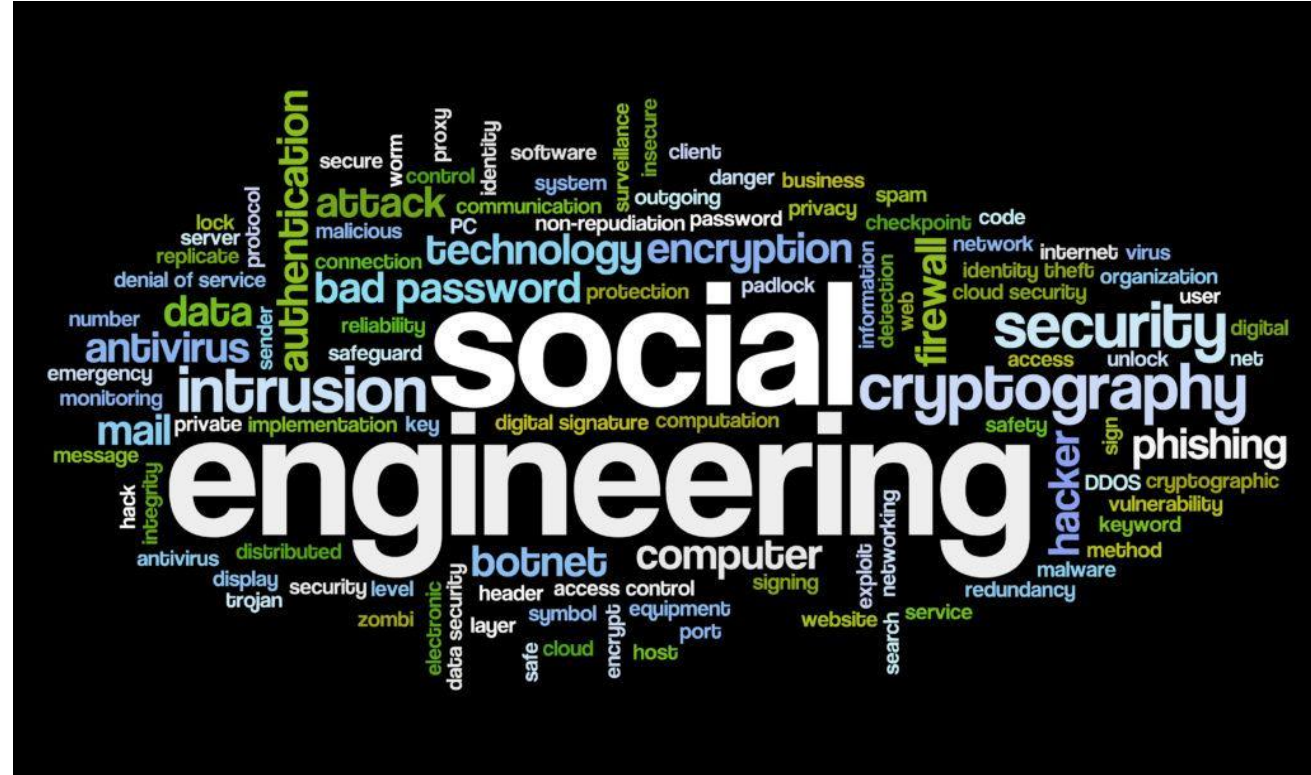


copyright 2006 John Klossner www.jklossner.com



- High quality **technology alone cannot keep data safe – why -** the human factor, **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)

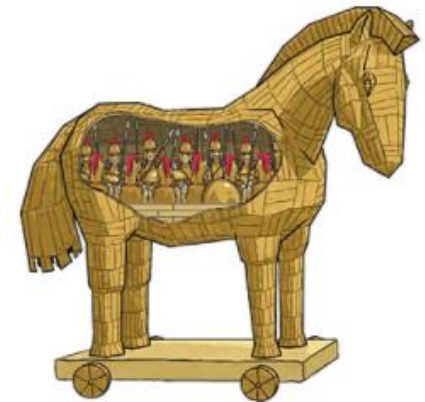


<https://threatpost.com/rethinking-responsibilities-social-engineering-attacks/148466/>

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



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



- **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**'

HQZ-888 Page 1 of 2



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

DATE: 03/16/2015

ACCOUNT NUMBER: [redacted]

COMPANY NAME: [redacted]

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

THANK YOU. WE APPRECIATE YOUR BUSINESS

PLEASE DETACH THE BOTTOM PORTION AND RETURN USING ENCLOSED ENVELOPE

- **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



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

DATE: 03/16/2015

ACCOUNT NUMBER: [redacted]

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.

HQZ-888 Page 1 of 2

Your mailbox is almost full



Microsoft Outlook

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.

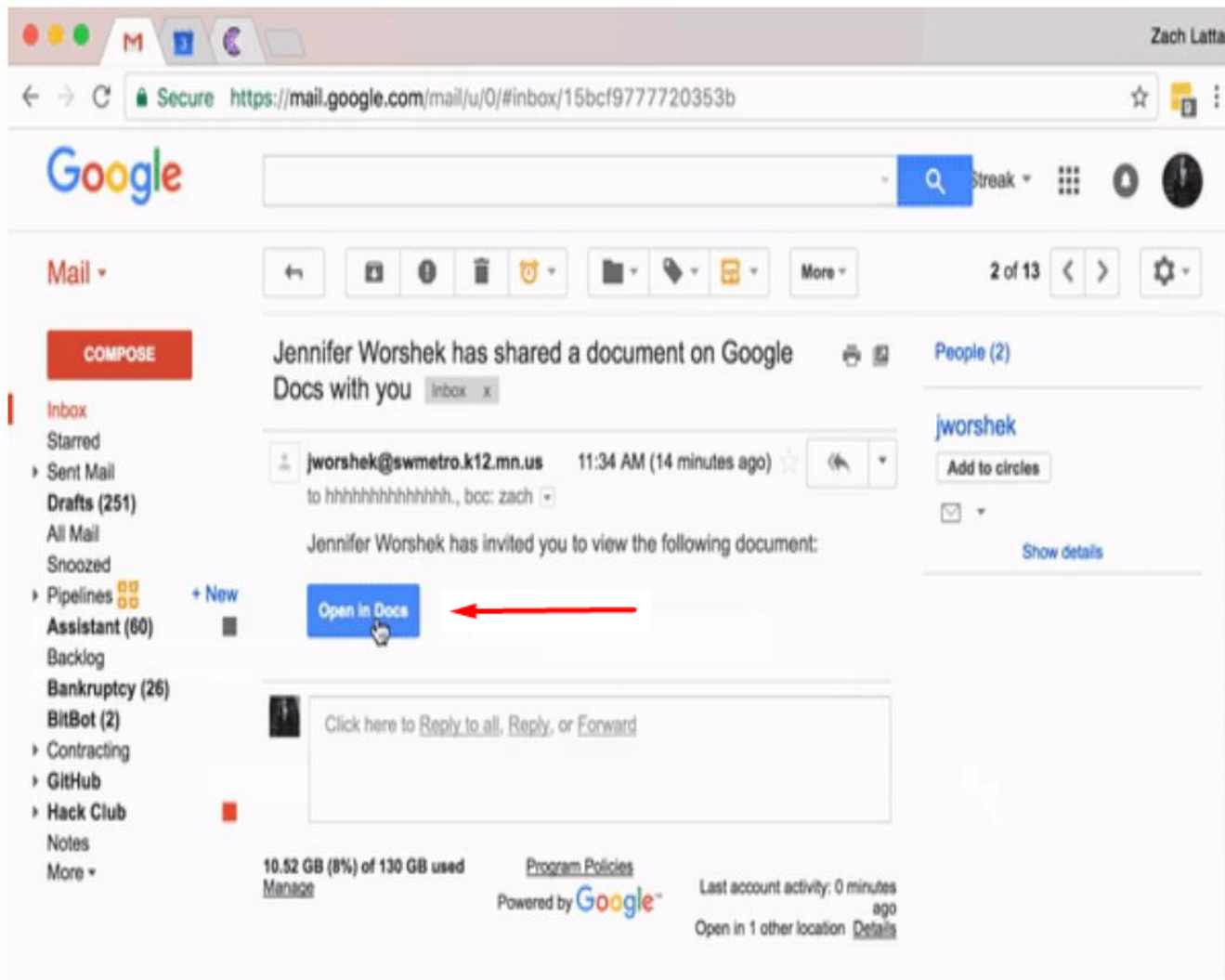
[Upgrade @.com](#)

Thanks,

message center



- 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




- 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



Welcome to Google Docs. Upload and Share Your Documents Securely
Sign in with your email address to view or download attachment

A login form for a phishing site. At the top is a grey circle with a white person icon. Below it is the text 'Select your email provider'. A dropdown menu shows 'Gmail' with the text 'Sign in with Gmail' and a downward arrow. Below the dropdown are two input fields: 'Email' and 'Password'. A blue button with white text says 'Sign in to view attachment'. At the bottom left is a checkbox labeled 'Stay signed in', and at the bottom right is a link that says 'Need help?'.

- 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

Drop-box 

 Junk

Document Received - (Scanned_Invoice90210.Pdf)

To: Rebekah Sack



You have a new document sent to you via Dropbox due to the large size of the file.

Sign in with your email to [View Document-Pdf 00874](#)

-Best Regards
Dropbox Team

- 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



CYBER GUARD DUTY: "DON'T CLICK THAT EMAIL KAREN!"

<https://www.darkreading.com/endpoint/beat-the-heat-dark-reading-caption-contest-winners>



<https://www.linkedin.com/pulse/cyber-security-healthcareis-industry-denial-miranda>

Overall Principle:

Access to data and resources to be based on work related 'need'

- **Policies need to be consistent with school culture, & based on consultation**

Different roles require different levels of access to data

- Principal, Deputy Principal
 - Administration Staff
 - Teachers, other staff
 - Students
 - Visitors
- **Segment the school network and wifi based on type of users**
 - Leadership/Admin, Staff, Students, Guest
 - This needs to be implemented on the school network
 - **Supports GDPR principles**
 - **Reduces risk of issues, data breach**

- **Access to data** and resources needs to be **restricted to those who really need it**
- **The number of data administrators** (ie 'admin accounts') **need to be minimized**
- **All 'admin accounts' need to be approved** by the School Principal
- **Data to be stored securely**
- **Robust data backups** to be in place

- **Possible examples:**
 - **Student devices** not to have access to Leadership/Admin or Staff network areas
 - **Policy on USBs** for staff and students- USBs to be used for school work only, AV Scan
 - Policy on school owned **teacher mobile devices**, to be used for school work only
 - Enforce **two factor authentication** (at least for staff)

- **Network and Wifi**
 - **Network to be segmented** either physically or by VLANs, and SSIDs for Wifi
 - Discuss this with your school network/wifi support provider, ETB

- **To reduce the risk of permanent loss of important school data** due to malware, equipment failure, or other causes, the **single most important step** that schools should have in place is to carry out **regular ‘standalone’ backups** of important school data.
- **A standalone backup** is one that is **stored in a separate, disconnected and/or ‘off-site’ location**, so that if the original data is lost or inaccessible, the **school still has a copy** of the data.
- The ‘standalone’ location could be a **separate drive** or could be on a **‘cloud based’ service**



<https://medium.com/technology-innovations-insights/what-impact-can-data-backup-and-recovery-trends-have-on-organizations-d65195a021b6>

- Ensure school **wifi is configured securely**
 - **Admin/Leadership, Staff, Student, Guest**
- Ask your **wifi provider / ETB to confirm this**
- **Switch off unused wireless connections** such as bluetooth connections
- **Install recommended software security updates** from Microsoft, Google, Apple etc.
- Microsoft's 'Windows 10' operating system (OS) includes AV software, however **it is still recommended to have to 3rd party malware/AV software** installed for Microsoft devices.
- **Risk to local servers, move to cloud services where possible**



<http://re-brostrand.com/secure-your-wi-fi-network/>



<https://www.sancuro.com/blog/post/why-software-updates-are-so-important/>

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

Danger Signs:- Delete emails without opening them if:

- You don't recognize the sender
- It's a generic/mass/bulk email
- It's not addressed to you
- 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, 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/>

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](#)

Online Scam Prevention

Follow these tips to avoid becoming a victim of an online scam.



Set up multi-factor authentication.



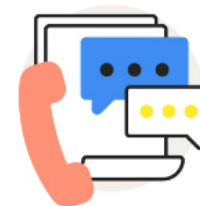
Never respond to scam messages.



Install antivirus software.



Keep social media accounts private.



File a complaint.



Be cautious transferring money.

Social Media Cleanup Checklist: A 9-step cybersecurity guide



- ✓ Find all of your social media accounts
- ✓ Make your accounts private
- ✓ Delete any inappropriate posts or comments
- ✓ 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

Public vs Private Social Media Accounts



Public

- Anyone can view your profile
- Anyone can comment on posts
- Posts can be shared anywhere



Private

- Manually approve followers
- Only followers see your posts
- Posts are hidden from searches

- **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 activated.**
- **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/>

- **In general Apple iPads cannot get viruses unless the user is jailbreaking, ie., downloading apps from outside of the Apple 'App Store'.**
- **If you're using iPads as intended and only downloading apps from the Apple App store, it's unlikely to get viruses.**
- **The reason why iPads do not get viruses is that every app in the App store is scanned for malicious code.**
- **Also each app is isolated from one another** so viruses can't spread to other systems
- **As with all other types of devices iPads can't protect users from Phishing, scams etc**
- **While it's unlikely that an iPad has a virus, it may be affected if for example, your mouse moves without you touching the trackpad, you are getting a lot of pop-ups, your passwords stop working, etc.**

<https://www.security.org/antivirus/ipads/>

- **Managing passwords is critical to cybersecurity**
Affects all computer based or online activities
- **No personal or social media passwords should 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 on 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

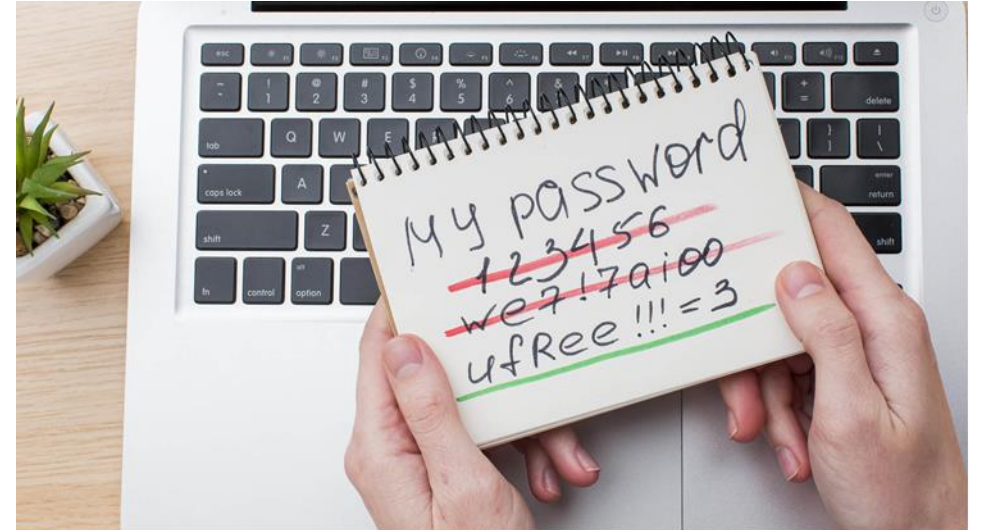
2-Step Verification

A text message with a 6-digit verification code was just sent to (...)70

Enter the code

G- 763076

- **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 words**, DOB, favourite teams, child or pet names, these can be easily found on social media
- Use **‘complexity’**: eg., include combinations, upper and lower case, numbers, special characters



<https://www.itekolutions.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:**

Examples:

LastPass: <https://lastpass.com/>

KeePass: <https://keepass.info/>

Keeper: <https://keepersecurity.com/>

Password Safe: <https://pwsafe.org/>

Dashlane: <https://dashlane.com/>

Ransomware tips:

Most of the ransomware attacks are linked to weak protection practices

- 1. Do not pay the ransom.** It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee of regaining access to your files.
- 2. If affected restore data from a known good backup.**
- 3. Do not provide personal information** when answering an email, unsolicited phone call, text message or instant message. Phishers will try to trick employees into installing malware, or gain intelligence for attacks by claiming to be from IT. Use reputable AV software and a firewall.
- 4. Make sure that all systems and software are up-to-date** with relevant patches.
- 5. Make sure you use a trustworthy Virtual Private Network (VPN) when accessing public Wi-Fi**

<https://us.norton.com/blog/emerging-threats/ransomware-what-can-you-do-about-it#>

- **Examples of ‘Trusted’ Websites**
 - etbi.ie
 - 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’ = secure) rather than just “http” or ‘www’.**

What Makes a Website Credible?



29.3%
A secure URL
(https)



18%
Testimonials
and reviews



7.3%
Trust badges



8.6%
Familiar methods
of payment

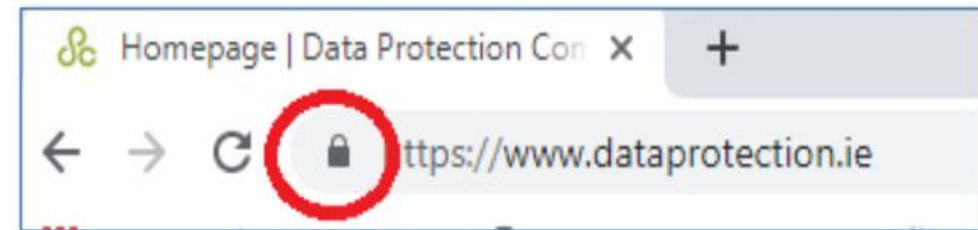


4.9%
Contact info



4.4%
Website design
looks professional

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



Types of incidents and level of support

- A cybersecurity incident is considered to be any adverse event that threatens the confidentiality, integrity, authenticity or availability of a network or information system.
- As a member of the public **if you feel that you have experienced a cyber security incident** that may have a national impact please contact the NCSC at the email info@ncsc.gov.ie.
- **The level of support given by NCSC will vary depending on the type and severity of the incident**, the constituent and/or constituents impacted and available resources.

Cybersecurity vs Cybercrime

- There are a number of cyber-related events which may not be considered as cyber security incidents but could constitute a cyber crime. **Cyber bullying, threats via email, text or instant message, online fraud or online extortion are all examples of potential cyber crimes.**
- If you feel you have been a victim of a cybercrime you should contact [An Garda Síochána](#).

Ransomware Support Website

- <https://www.nomoreransom.org/>
- If you feel you have been a victim of Ransomware you should contact [An Garda Síochána](#).





Network Security: Fit for purpose **router and firewall in place** to prevent unauthorised access and malicious content.



User Awareness: Produce security policies detailing the correct and secure use of devices and online systems. Regular cyber security awareness training.



Malware Prevention: Produce appropriate policies on malware, install anti-virus protection on the school's devices. Disable USB ports unless strictly necessary.



Account Security: Manage and limit user access as well as monitoring user activity. Create a **password policy**. Recommend strong and unique passwords for accounts and services. Consider using a password manager to store passwords. Enable **multi-factor authentication (MFA)** on all accounts if possible.



Backups: Create backups regularly and **consider a cloud solution**. Have policy to **control all access to removeable media, limit media types and scan media before importing onto the network**. Apply software updates as they become available.



Prepare: Develop an **incident plan** and involve staff. Document contact details of external people who can help during an incident. Monitor systems and network for unusual activity.

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

Citizensinformation.ie

[How to avoid scams \(citizensinformation.ie\)](https://www.citizensinformation.ie/en/your_rights/avoiding_fraud/avoiding_fraud.html)

PDST-TiE

[Data and Cybersecurity - PDST Technology in Education](https://www.pdst.ie/technology-in-education/data-and-cybersecurity)

Cyberwise (Involving students)

<https://cyberwise.ie/>

Some 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/>

Cyberwise

Cyber Resilience Education in Primary and Post-Primary Schools

Welcome to cyberwise.ie. Here you will find information and resources on the Junior Cycle Cyber Security Short Course.

<https://cyberwise.ie/>

- **Objective: Build a positive culture among staff, students of securely managing data**
- **Review current school situation**, including policies and procedures
- **Talk to your ETB** to understand what advice, support and services are available for the school to build a positive cybersecurity culture
- **Training on Cybersecurity**
 - Use references (ETB, NCSC, PDST-TiE, Garda etc) for advice and support
 - Implement relevant policies, train key staff (and some students) initially
 - Wider staff and student training, **seek feedback on what works, seek to innovate!**
 - Involve students, integrate student activities into specific subjects areas
- **Ongoing review and update** of policies, procedures, training as required, sessions for staff and students
- **Seek ongoing support from** your ETB as necessary

PDST Technology in Education

<https://www.pdsttechnologyineducation.ie/technology-infrastructure/>

Please send any queries to ictadvice@pdst.ie