

# Cybersecurity Awareness and Guidance for the School Leadership Team

July 2025

[Oide Technology in Education Website](https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/)

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

Email: [ictadvice@oide.ie](mailto:ictadvice@oide.ie)

- 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?
- Guidance on how schools can reduce these risks
- Some relevant resources, links etc.,

- 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>

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
- 31<sup>st</sup> 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**

## 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 policies 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'**

- 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 ransomware attack will have a major negative impact on a school**





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

**RANSOMWARE**



Blackmails you

**SPYWARE**



Steals your data

**ADWARE**



Spams you with ads

## Types of Malware

**WORMS**



Spread across computers

**TROJANS**



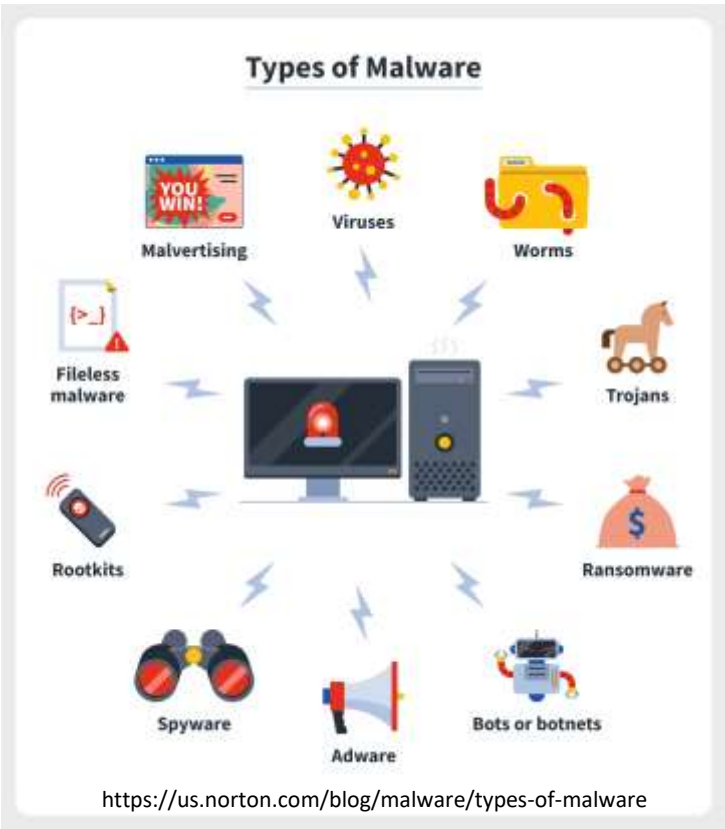
Sneak malware onto your PC

**BOTNETS**




Turn your PC into a zombie

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



## Zero-Day

**ZERO-DAY VULNERABILITY:**  
**THE UNKNOWN THREATS TO YOUR DATA**



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



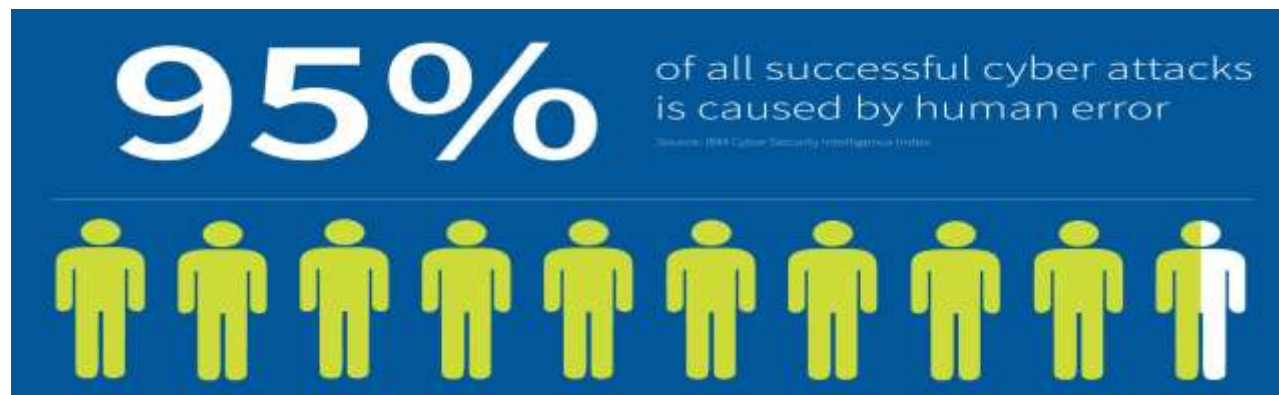
<https://www.g2.com/articles/spoofing>

## Identity Theft

## Ransomware



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



<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



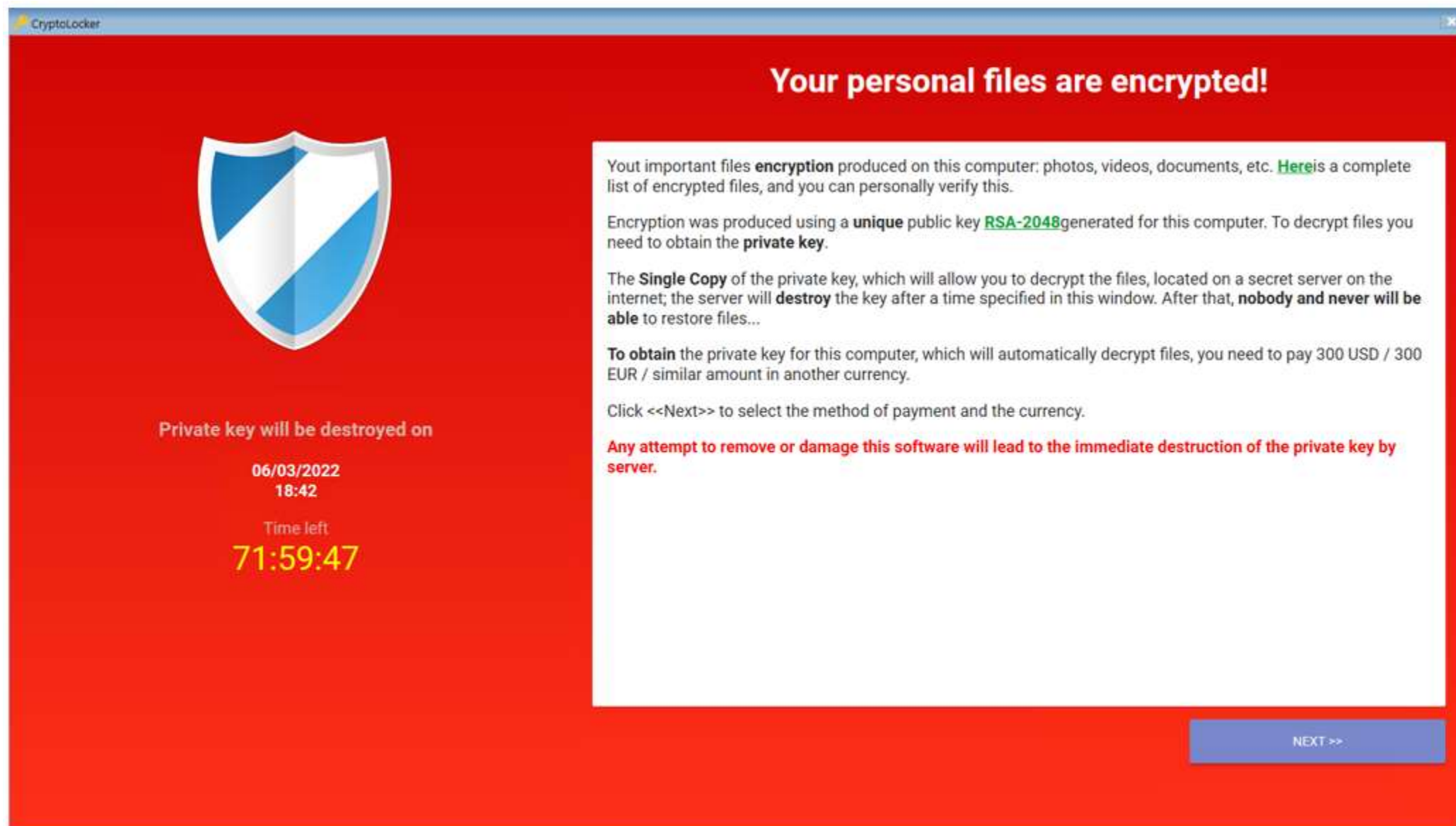
<https://enterpriseproject.com/article/2016/2/internet-hackable-things-why-iot-devices-need-better-security>



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

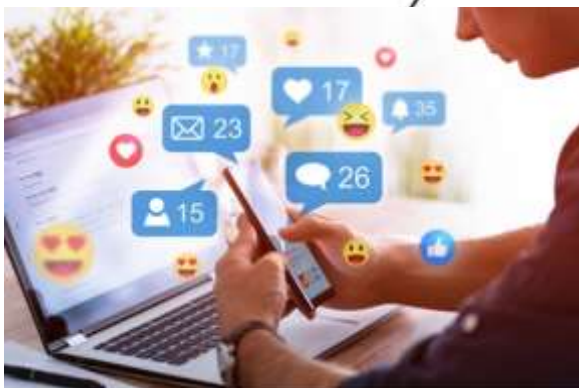


# Impact of Ransomware



- **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/school accounts

Personal

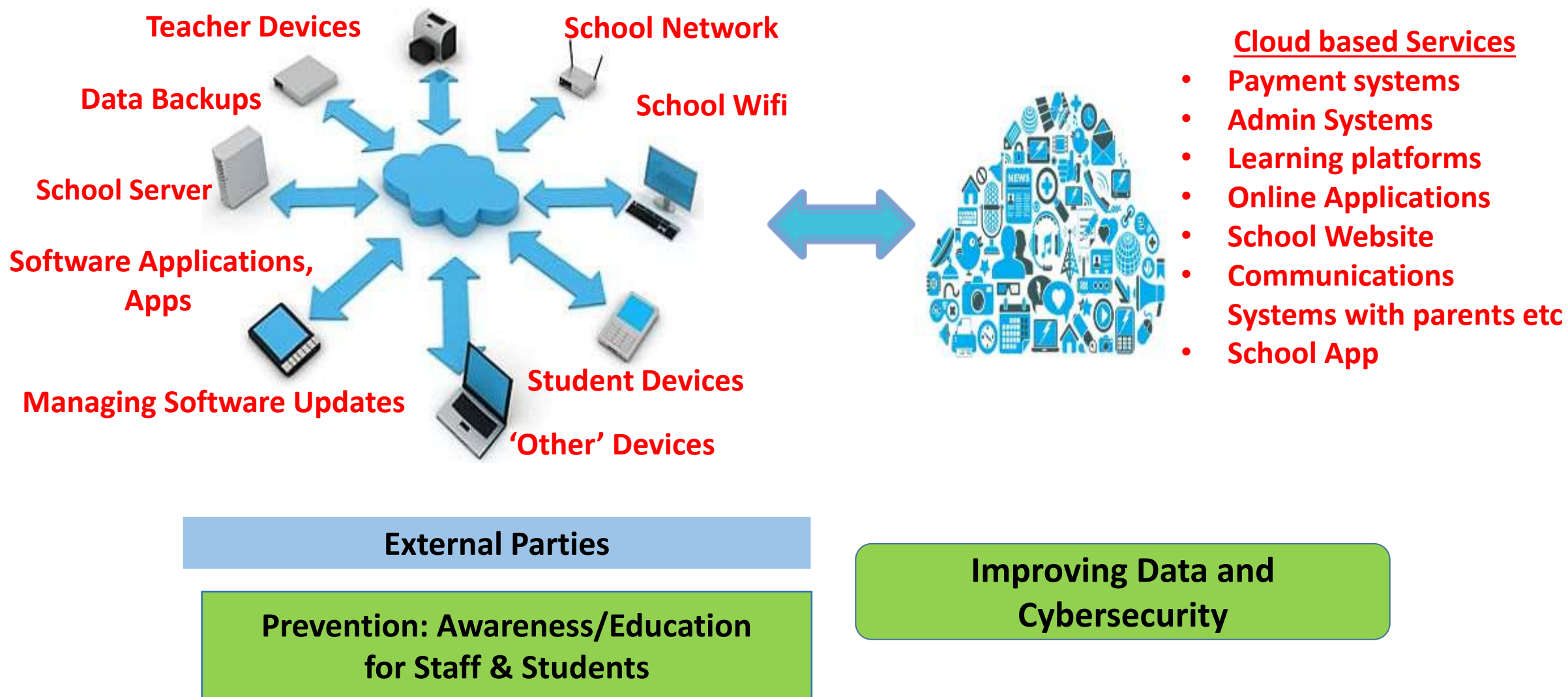


<https://www.insurancebusinessmag.com/us/news/cyber/social-media-activity-exposing-many-users-to-cyber-risks--report-245417.aspx>

Work/School



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





- **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](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 ...

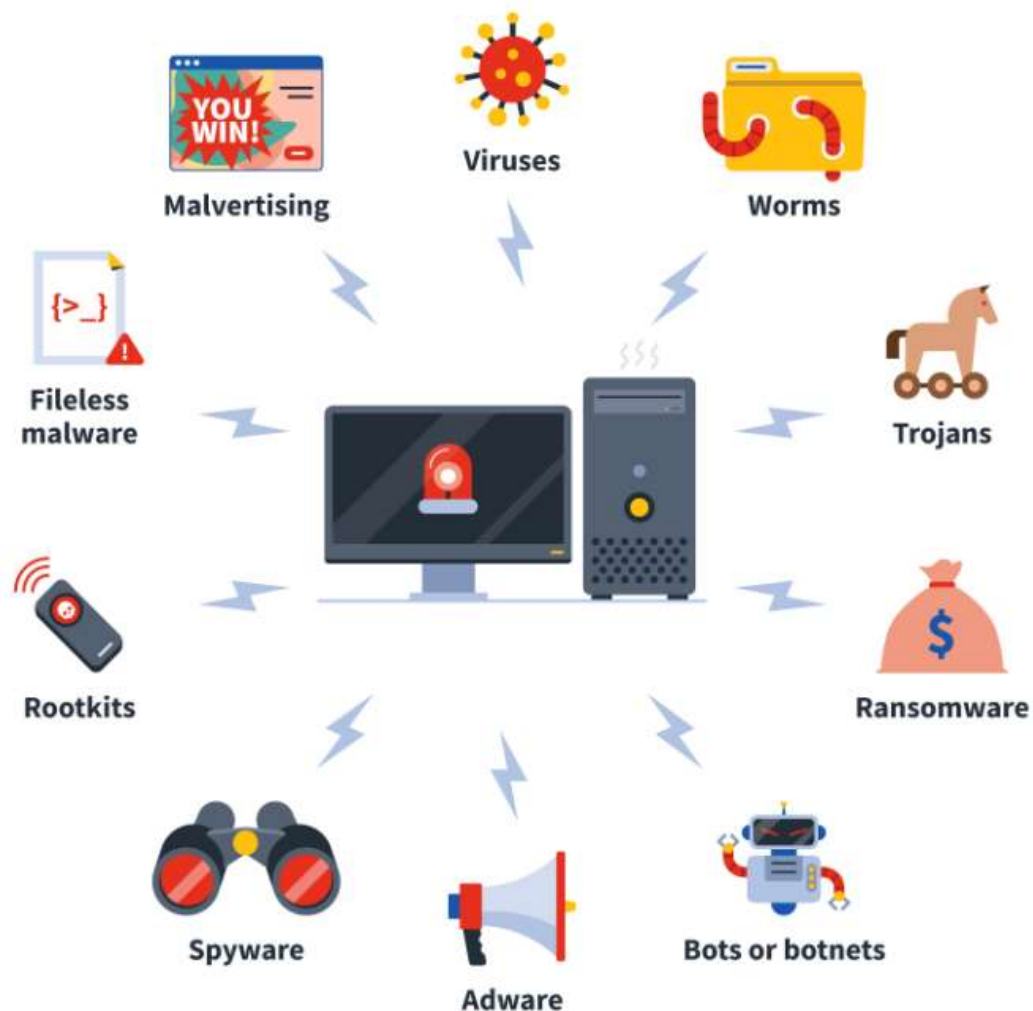
## Viruses – Need for AV on different types of devices

- **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.**

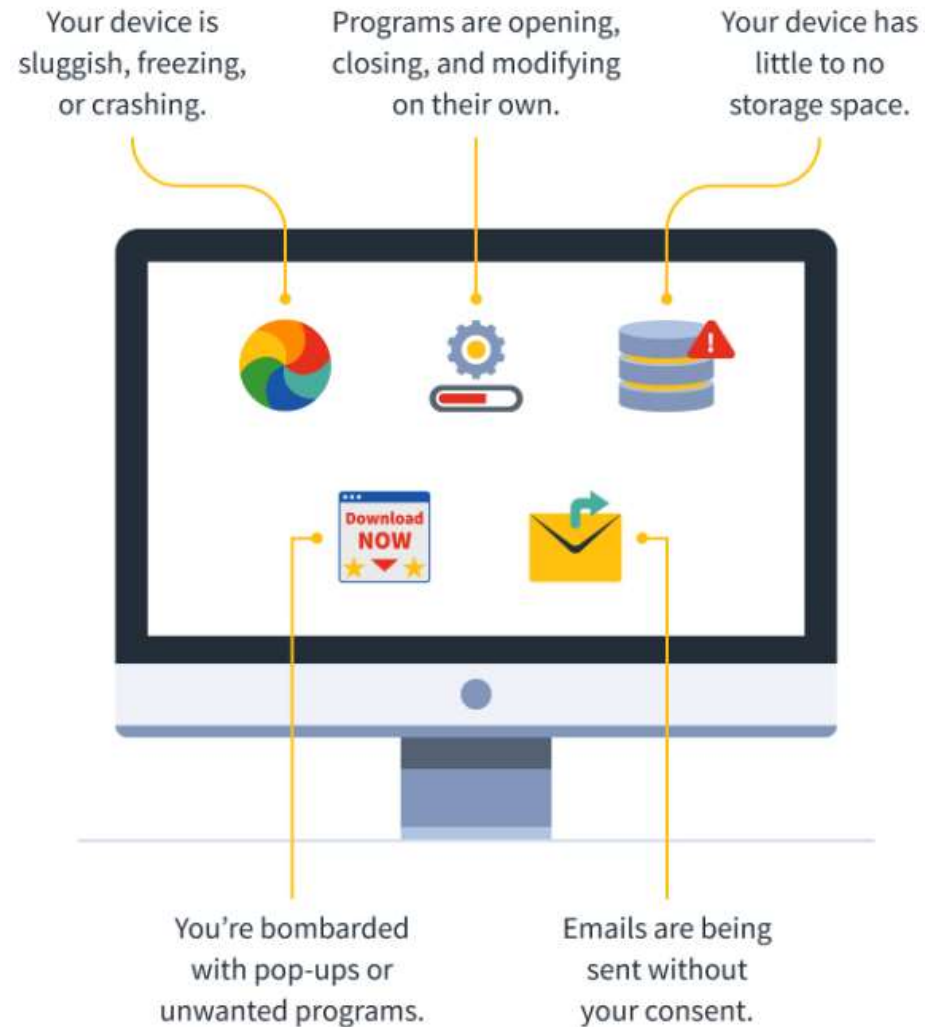
<https://www.security.org/antivirus/>



## Types of Malware



## The Warning Signs of Malware



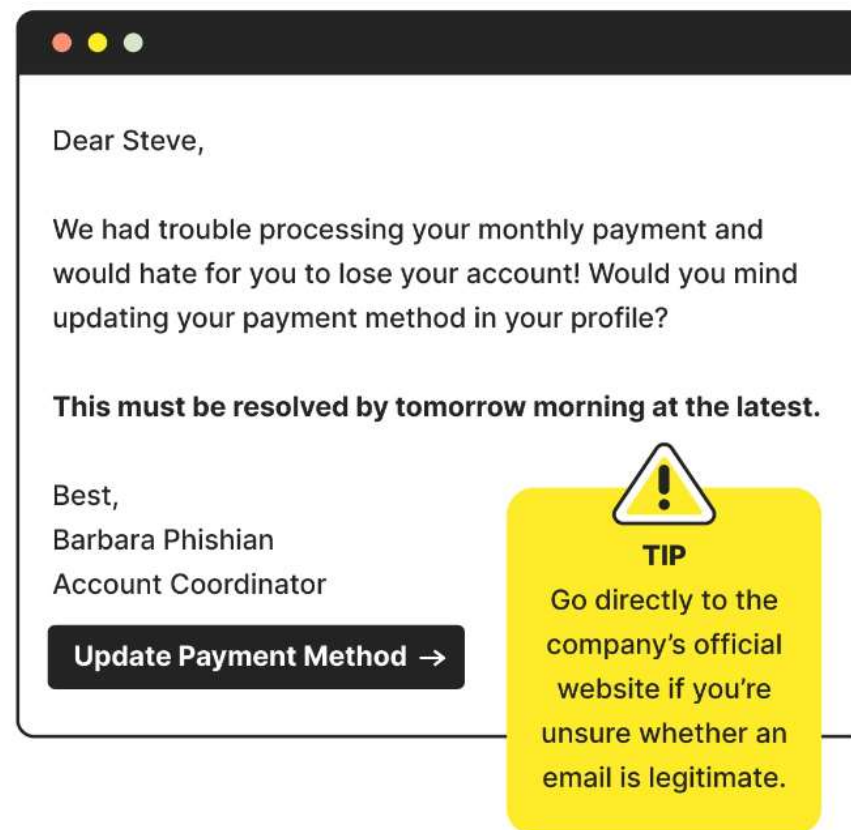
- [illegible]

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

- **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](https://www.infosecinstitute.com/what-is-phishing/), **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: (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 3<sup>rd</sup> 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**'



# Phishing Invoice attack

HQZ-888 Page 1 of 2



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

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

THANK YOU, WE APPRECIATE YOUR BUSINESS

PLEASE DETACH THE BOTTOM PORTION AND RETURN USING ENCLOSED ENVELOPE



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

03/16/2015

ACCOUNT NUMBER

AMOUNT \$70.00

AMOUNT ENCLOSED \$

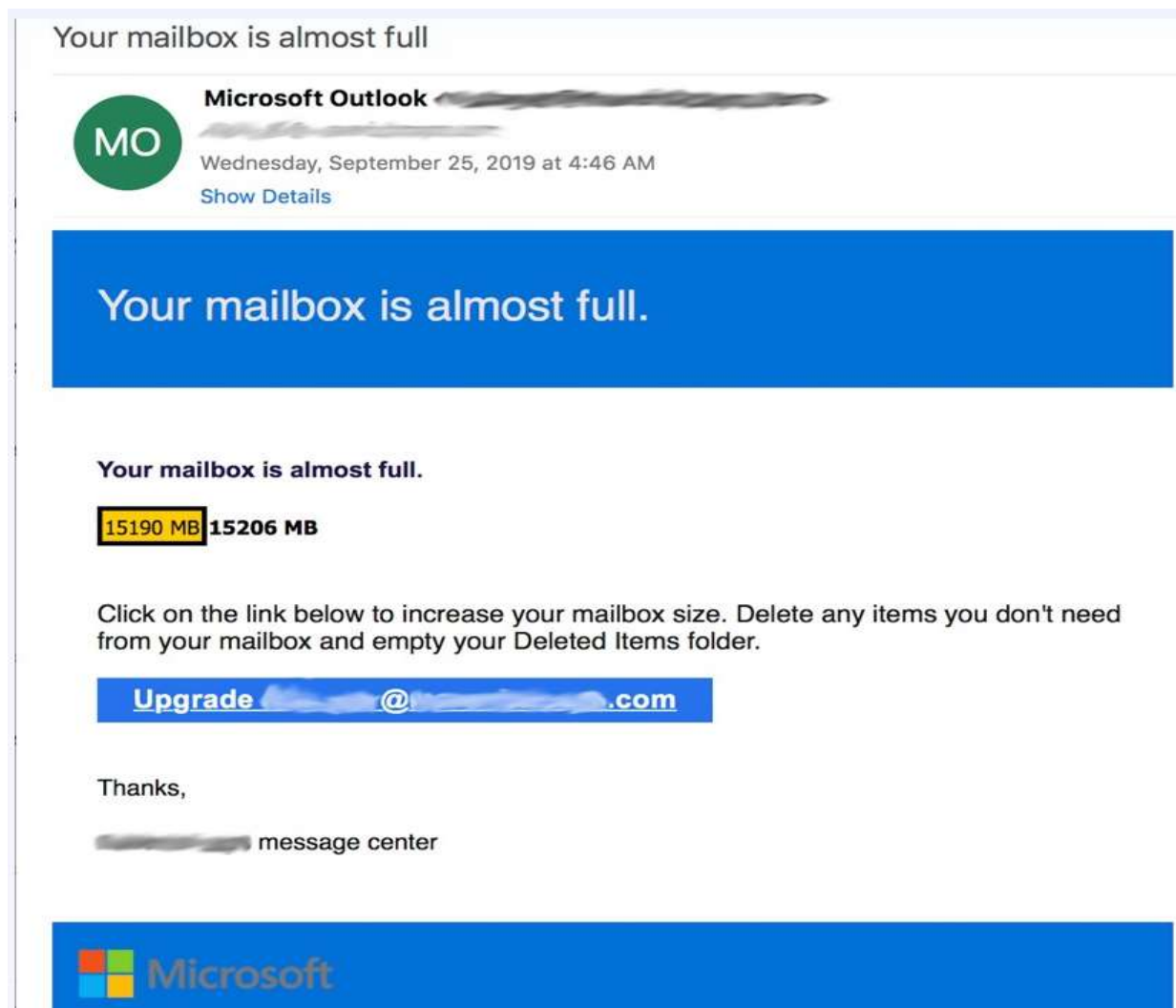
PAY BY CHECK OR MONEY ORDER ONLY.  
Make payable to WEBSITEBACKUP COMPANY and include your account number on it. All checks will be deposited upon receipt. DO NOT SEND CASH OR POST-DATED CHECKS.

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


HQZ-888 Page 1 of 2

- **Phishing** - method of accessing data using social engineering / deception
- Email with **attached Invoice** from a 3<sup>rd</sup> 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 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

Drop-box 

 Junk

Document Received - (Scanned\_Invoice90210.Pdf)

To: Rebekah Sack

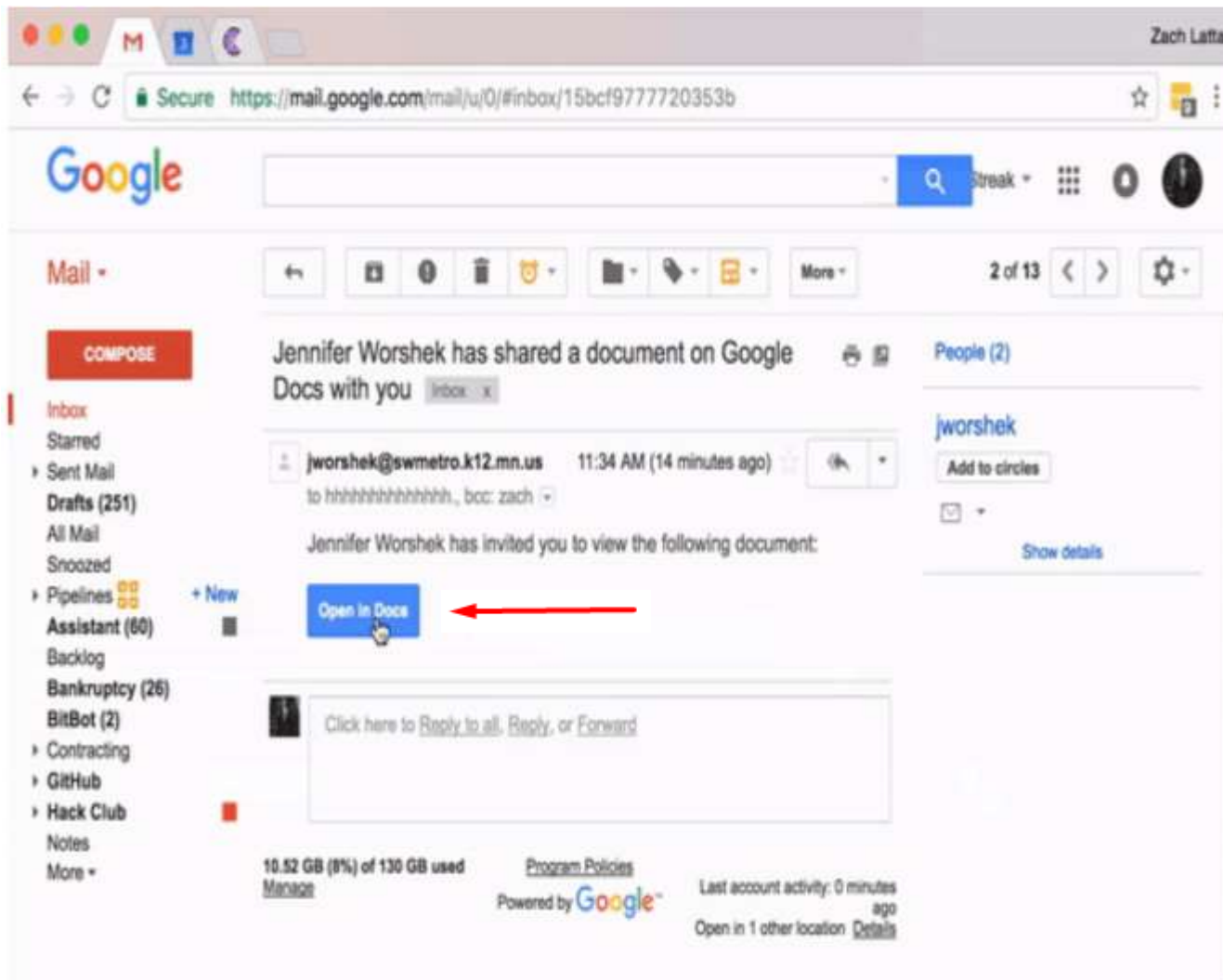


You have a new document sent to you via Dropbox due to the large size of the file.

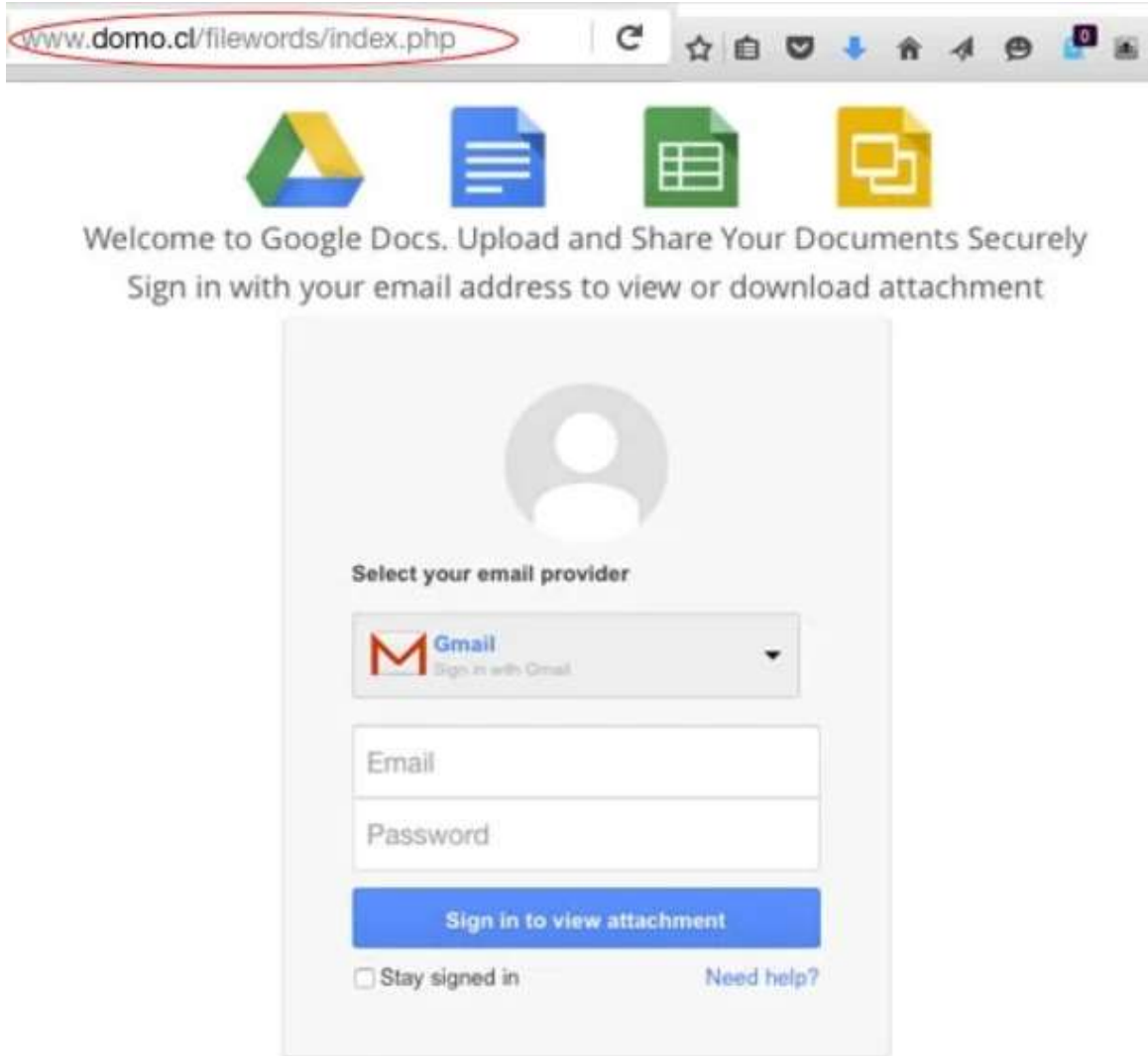
Sign in with your email to [View Document-Pdf 00874](#)

-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



- 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



- 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

**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 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/>

**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

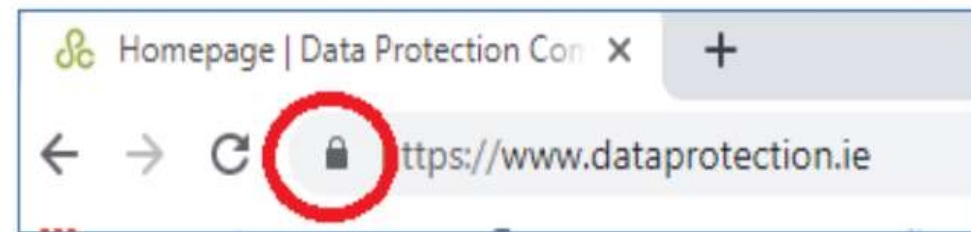
- Manually approve followers
- Only followers see your posts
- Posts are hidden from searches

- **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’.**

## What Makes a Website Credible?



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



## 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 - USBs to be used for school work only, AV Scan
  - Policy on USBs for students - USB to be used for school work only, AV scan
  - Policy on school owned teacher mobile devices, to be used for school work only
  - Consider enforcing two factor authentication (at least for staff)
- Network and Wifi
  - **Network to be segmented** either physically or by VLANs, and SSIDs for Wifi
    - to be discussed with your school network/wifi support provider

## Importance of standalone data backups

- 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 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 3<sup>rd</sup> party malware/AV software** installed for Microsoft devices.



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



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



## 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/>

# iPads and Viruses

- In general Apple iPads cannot get viruses unless the user is jailbreaking, meaning is downloading apps from outside of the App Store.
- If you're using iPads as intended and only downloading apps from the 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, **you can tell if it has a virus if** 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/>

## Tips re' Ransomware

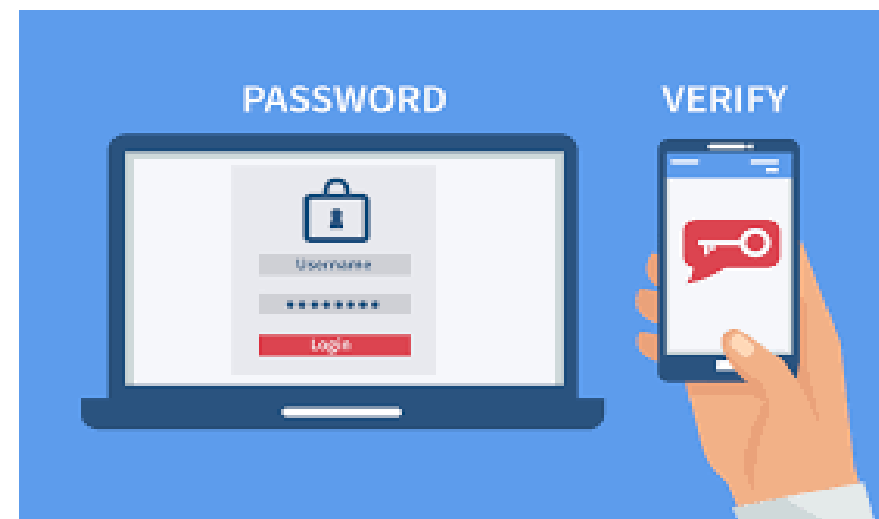
### Ransomware tips:

Most of the ransomware attacks are linked to poor protection practices by employees.

1. **Do not pay the ransom.** It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
2. Restore impacted files **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#>

- **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

### 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, dictionary words, DOB, 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](#)

# Reporting a data breach to DPC



[YOUR DATA](#) [FOR ORGANISATIONS](#) [RESOURCES](#) [WHO WE ARE](#) [NEWS AND MEDIA](#) [DATA PROTECTION OFFICERS](#)

## Report a Breach Of Personal Data

There is an **obligation**, in certain circumstances, on **organisations** to file a report with the DPC. Use this form if you wish to contact us on behalf of an **organisation** to report a personal data breach\* that has occurred in your organisation (or that you think may have occurred), in circumstances where you have determined that the **breach presents a risk to the affected individuals**.



CONTACT THE DPC

### For Organisations

REPORT A BREACH

REGISTER YOUR DPO

<https://www.dataprotection.ie/>



# Reporting Cybersecurity Incidents and Crimes

## 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](mailto: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](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](mailto:ictadvice@oide.ie)