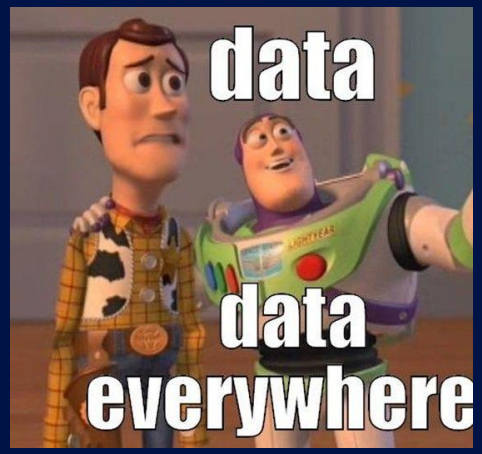
Cybersecurity Training

STETSON cybergroup

What is Cybersecurity and Why it is important for Education?



Definition: Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

- Cybersecurity is important because education organizations collect, process, and store unprecedented amounts of **data** on computers and other devices for students, parents, teachers, administrators, office staff, and others.
- Data in education includes personally identifiable information (PII).
- Examples of PII include, but are not limited to:
  - Full Name, Email Address, Home Address, Date of Birth, National ID numbers / Social Security number, Salary, Place of Birth, Insurance details, Medical information, Credit score / record, Criminal record, And more…
- Schools also must protect data related to Personal Health Information (PHI) and Individualized Education Program (IEP) in accordance with Family Educational Rights Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA) regulations.

Non-Technology Reasons Education is at Risk

- Schools store vast amounts of personally identifiable information (PII), including student records, financial data, and personnel information, making them attractive targets for cybercriminals.
- Schools often operate with limited budgets and resources, leading to outdated IT infrastructure and insufficient cybersecurity measures.
- Faculty, staff, and students lack training to spot and report cyberattacks.
- As schools become increasingly interconnected through technology adoption, exposure to threats and vulnerabilities increases.
- Students, faculty, staff, or contractors may misuse their user privileges — intentionally or by mistake — to gain unauthorized access to sensitive data and systems.

How Education is Targeted

Phishing, Vishing, Smishing, and Quishing are highlighted as the top threats facing education, suggesting hackers regularly target the sector using the method.

- **Phishing** – Phishing scams often take the form of an email or instant message and are designed to trick the user into trusting the source in a fraudulent attempt to access their credentials – whether that's sensitive student data or confidential research.
- **Vishing** – is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.
  - **Latest phone scam has bogus caller recording your voice and using the recording of "Yes", "No", and other words to steal your identity.**
- **Smishing** - the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.
- **Quishing** - is a form of phishing attack that uses QR codes instead of text-based links in emails, digital platforms or on physical items.
  - **Quishing is a social engineering technique used by scammers and cybercriminals to trick you into providing personal information or downloading malware onto your device.**

SCAN ME

What has Changed in 30 Years?

- Initially, hackers were either individuals or small groups targeting specific companies for personal gain.
- However, as time passed, we've witnessed the emergence of **nation-states** deploying **armies of hackers** to steal data, information, and money from a wide range of organizations.
- The 2023 FBI Internet Crime Report revealed staggering losses of over $12.5 billion, with 14 out of 16 critical sectors experiencing at least one member falling victim to a ransomware attack.
- **Great concern among most government agencies regarding the vulnerability of infrastructure (the rail network, aviation, drinking water, wastewater and energy).**
- This is concerning, especially given the multitude of Federal and State regulations and frameworks surrounding cybersecurity and data protection!

Business Email Compromise

- A type of cybercrime where the scammer uses email to trick someone into sending money or divulging confidential info.
- The culprit poses as a trusted figure, then asks for a fake bill to be paid or for sensitive data they can use in another scam.
- **Anyone** can be the target of a **BEC** scam!
  - **Data Theft** - Sometimes scammers start by targeting the HR department and stealing company information like someone's schedule or personal phone number. Then it's easier to carry out one of the other BEC scams and make it seem more believable.
  - **False Invoice Scheme** - Posing as a legitimate vendor your district works with, the scammer emails a fake bill/invoice—often closely resembling a real one. The account number might only be one digit off. Or they may ask you to pay a different bank, claiming your bank is being audited.
  - **School Administration/School Board Fraud** - Scammers either spoof or hack into an email account, then email employees' instructions to make a purchase or send money via wire transfer. The scammer might even ask an employee to purchase gift cards, then request photos of serial numbers.
  - **Account Compromise** - Scammers use phishing or malware to get access to a finance employee's email account, such as an accounts receivable manager. Then the scammer emails the suppliers fake invoices that request payment to a fraudulent bank account.
- If a business email compromise attack is successful, your district could:
  - Lose hundreds of thousands to millions of dollars.
  - Face widespread identity theft if personally identifiable information is stolen.
  - Accidentally leak confidential data like intellectual property.
  - Get shut down for days, weeks, or months!

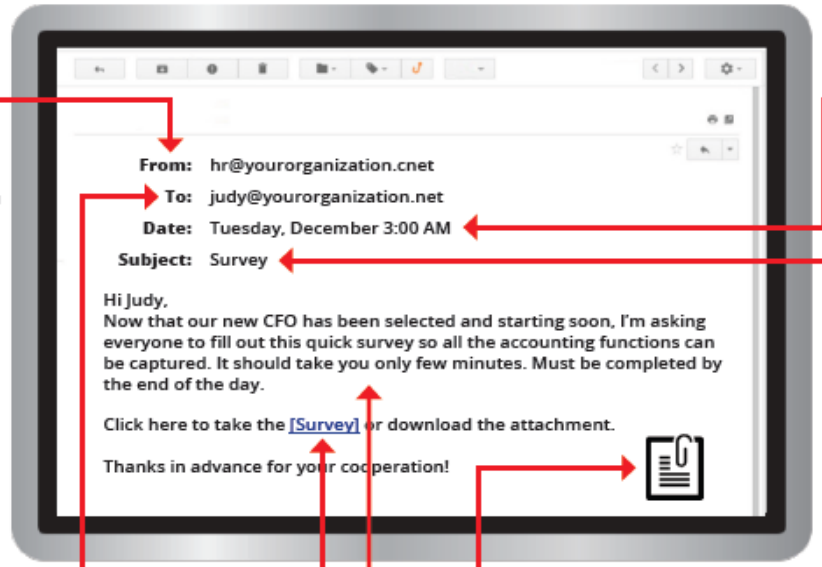
Business Email Compromise Examples

- Example #1: Pay this urgent bill!
  - Say you work in your district's finance department. You get an email from Administration with an urgent request about an overdue bill—but it's not actually from Administration. Or the scammer pretends to be your repair company or internet provider and emails a convincing-looking invoice.
- Example #2: What's your phone number?
  - A vendor emails you, "I need your help with a quick task. Send me your phone number and I'll text you." Texting feels safer and more personal than email, so the scammer hopes you'll text them payment info or other sensitive information. This is called "smishing," or phishing via SMS (text) message.
- Example #3: Your lease / software license is expiring
  - A scammer gets access to an organization's email, then finds transactions in progress. They email clients, "Here's the bill to renew your lease / software license for another year" or "Here's the link to pay your subscription." Scammers recently swindled someone out of more than $500,000 this way.

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known website. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

New York State Education Department

- New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information.
  - (a) As required by Education Law §2-d (5), the Department adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the standard for data security and privacy for educational agencies.
  - (b) No later than July 1, 2020, each educational agency shall adopt and publish a data security and privacy policy that implements the requirements of this Part and aligns with the NIST CSF.
- Some requirements of the NIST CSF School Districts must implement:
  - Protect Physical Assets
  - Manage Access to Systems
  - Implement Multi-Factor Authentication
  - Users are Trained at least annually

New York State Education Department

- Educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data.
  - Parents bill of rights for data privacy and security.
    - A parent's bill of rights for data privacy and security shall be published on the website of each educational agency and shall be included with every contract an educational agency enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data.
    - Enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights.

Phishing Emails

How many click on links in malicious emails are too many clicks?

Answer on next slide…

ANSWER:

Who is responsible for Cybersecurity at Hempstead?

EVERYONE!

With cybersecurity training, and simulated phishing attacks to increase the awareness on the motives and method of attackers, education venues could better protect themselves against cyberattacks.

2023 - 2024 Cybersecurity Attacks on Education

- For the period from 2016-2021, there were over **1,600 publicly-disclosed** incidents affecting U.S. School Districts (and other educational organizations) across ALL 50 states.
- From January 2023 through June 2024, at least 83 potential ransomware attacks on school districts were disclosed.
- In 2023, 35 Long Island school districts suffered from cyber incidents.
- 2023 Most Notable Education Hacks:
  - MOVEit breach - MOVEit is a file-transfer platform used by thousands of governments, financial institutions, and other public- and private-sector organizations around the world. In May, the platform was hacked in a breach believed to have affected at least 161 U.S. schools.
  - **New Haven Public Schools, Conn.** – In May 2023, the New Haven school district in Connecticut lost more than $6 million after hackers appeared to have gained access to the email account of the district's chief operating officer. The hackers monitored the email correspondence between the COO and vendors and eventually impersonated both to divert district payments to its school bus contractor and a law firm to fraudulent accounts.
  - **Prince George's County Public Schools, Md.** – August 14, 2023, about 4,500 user accounts were impacted by a ransomware cyberattack, the majority of which were staff accounts.
- May 2024, Mineola School District was hit with a cyberattack that caused internet and phone outage.

At Work or At Home – Cyber Education

- **Human element** is still very much the driving force behind an overwhelming majority of cybersecurity problems.
- More than two-thirds of all data breaches are caused by non-malicious human elements.
- Cybersecurity training is important to the success of any school district. Advancements in technology continue to drive better productivity and efficiency levels, especially for school district employees. However, these same advancements have also left organizations vulnerable to more advanced forms of cyber attacks.
- Embrace Education and Training!
  - As the first line of defense, employees play a vital role in keeping school districts safe from malicious sources. Therefore, cybersecurity training is now a vital part of district-wide operations and requires active steps to manage properly.
  - Security & awareness training, also referred to as cyber awareness training, is the process of formally educating a workforce on the various cyber threats (e.g. - phishing, smishing, vishing) that exist, how to recognize them, and steps to take to keep themselves and their organization safe.
  - Cyber awareness training is typically approached as a long-term strategy and part of a larger security program.

Annual Cybersecurity Education & Training – WHY???

- Learning computer security not only works but protects your work and home accounts.
  - Drives awareness - A solid security awareness training program will drive cyber awareness and instill the knowledge and confidence in employees to recognize security threats when they're presented and how to properly respond and escalate the issue.

  - Reduces Threats - With a cyber awareness program, employees will be mindful of information security best practices as they pertain to regularly consumed applications and technologies in the workplace, including social media, email, and websites.
  - Prevents downtime - If your employees are familiar with cybersecurity principles and understand their role in keeping your business secure, there is far less likelihood that a cyber attack will take place and all critical systems can remain online and functional.

At Work or At Home – Password Don'ts!

DON'T

- Use the same password for numerous accounts.
- Include your favorite sport or hobby.
- Share your password with anyone.
- Include **easy** Sequences
  - (i.e. -1234 or ABCD).
- Write down your password and leave it in plain sight.

At Work or At Home – Password Do's!

DO

- Use long (minimum 12 character) AND complex (numbers, upper and lowercase letters, and symbols).
- Update/change passwords often.
- Avoid storing passwords on easily accessible devices or written under keyboards.
- Use a password manager (app on phone and/or extension on web browser).
  - Keeper and 1Password are highly recommended.
- Use MFA!!!

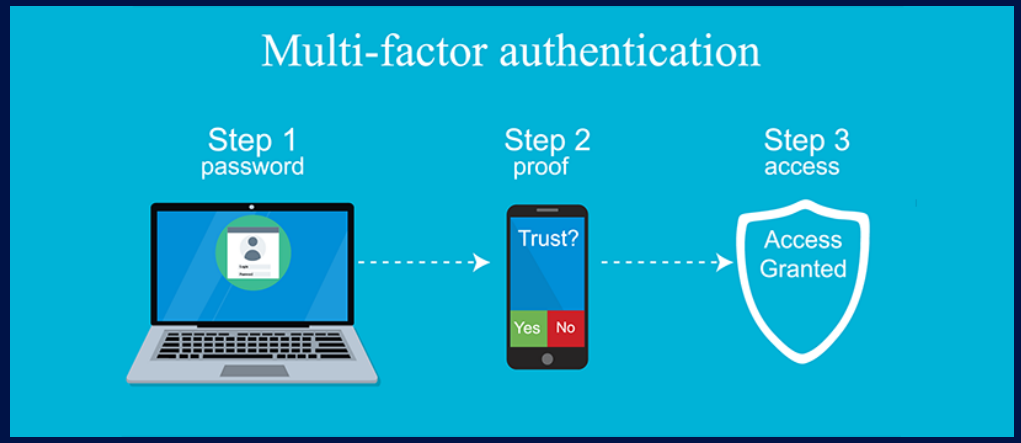
At Work or At Home – Password Do's!

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

At Work or At Home - MFA

- Use Multi-Factor Authentication (MFA) for all applicable devices
  - Multi-factor authentication (MFA) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).



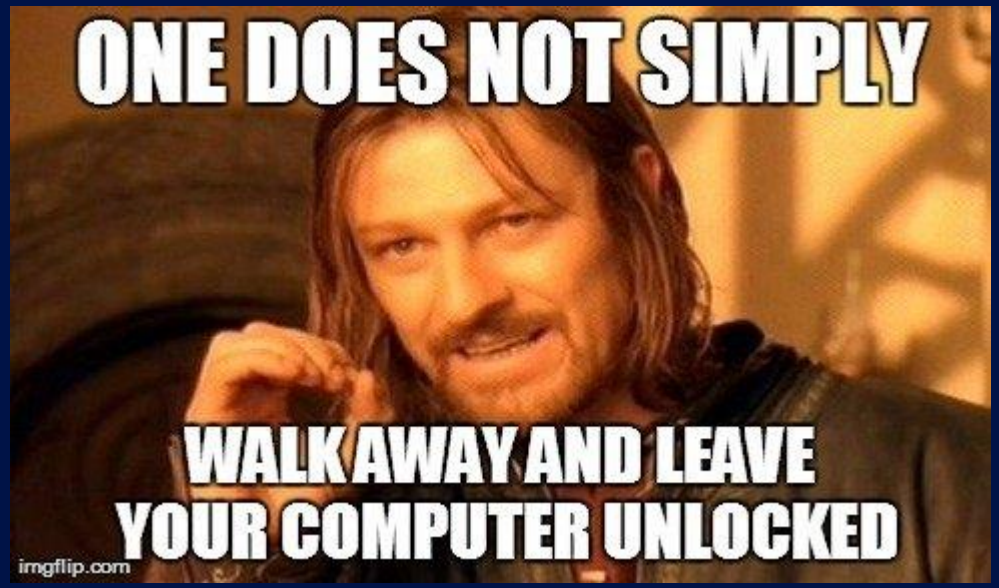
  - MFA adds an **extra layer of security** to such applications using time-based one-time password (TOTP) via call or SMS, Google Authenticator, etc.
  - MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

At Work or At Home - Mobile Devices

- Use Strong Authentication
  - Enforce strong login passwords/PINs for the device; PINs should be at least six digits.
  - Enable two-factor authentication (2FA). 2FA options pair a password or PIN with another form of authentication, such as a rotating passcode, SMS message, or biometric input.
  - For maximum protection, enable the use of biometric authentication (face or fingerprint).
- Update Your Mobile Operating System (OS) and Apps
  - Outdated OS and apps can be full of vulnerabilities and security flaws that could allow hackers to access your device.
  - Updates provide the latest security patches for your device and fix those security flaws.
- Have a screen time out set for your phone
  - Automatically lock your phone so all information is no longer available when you put down your phone or forget to take it with you.
- Turn Off Bluetooth when Not in Use / Monitor devices connecting to Bluetooth
  - Minimizing your Bluetooth usage minimizes your exposure to very real vulnerabilities.
- Avoid using unsecured public Wi-Fi networks
  - Hackers can also use an unsecured Wi-Fi connection to distribute malware.
  - If you allow file-sharing across a network, the hacker can easily plant infected software on your computer.

At Work or At Home – Physical Security

- Shut down your computer or device whenever you leave your seat, office, or classroom…**Windows + L**
  - It helps to protect confidential communications. Sometimes somebody may send you confidential information that is supposed to be for your eyes only. (e.g. – Student PII, Teacher Social Security #, Bank Account #, Medical Info, etc.)
  - Even if you're only popping by the kitchen for a cup of tea, or a quick bathroom break – Lock your computer so its not open to anyone, with all your documents, files, confidential information at hand.



At Work or At Home – Physical Security

- Don't Allow any Tailgating
  - Tailgating is a simple social engineering attack enabling hackers to gain access to a password-protected or otherwise off-limits physical location.
  - Tailgating involves closely following an authorized person into a restricted access area. As an employee opens a heavy door, for example, a tailgating social engineer may grab the door as it's about to close, walking right into the targeted physical system.

At Work or At Home – Physical Security

- Maintain a Clean Desk
  - Before leaving for the day, clear your desk and make sure all confidential and/or sensitive information is locked away.
  - Keeping Sensitive Information Under Control. The most significant benefit of having a clean desk policy is that you'll control and prevent sensitive information from falling into the wrong hands.

At Work or At Home – Computer Safety

- Never download any unauthorized / unapproved / unknown software.
  - Increases risk of malware and viruses infecting your desktop, laptop, Chromebook, mobile device (phone, tablet, etc.), and any other device connected to the network and/or WiFi.
  - Your District maintains a list of approved software for use.
  - Any software not on the approved list should be vetted with IT before downloading.
- Update Operating System and or Software on all your devices when prompted.
  - These software updates are an important part of maintaining the security of your applications and software.
  - With every software update comes change(s) that will improve the performance of your product by fixing minor issues that have been found and deemed possibly penetrable by threats.
  - Hackers thrive off their ability to enter any system weaknesses to take advantage of the data and information they can receive from it.
- Never plug unknown USB Flash Drives into your device.
  - It may consist of malware that could infect your devices.
  - It could also steal and damage PII and personal information.
  - If you find a USB on school grounds, it's wise to report it to your IT department.

We've Been Hacked, Now What Do We Do?

- At work, if you suspect you are the victim of an event / incident, **STOP** using your device.
  - Disconnect your device from the network…**DO NOT** turn it off! Turn off the WiFi or place device in Airplane mode. When applicable, unplug the network cable immediately.
  - The less you use the device, the easier it will be for IT or investigators to identify the source.
- Contact your local IT department **IMMEDIATELY**.
  - Always keep the phone numbers of the IT department's Help Desk and key IT contacts nearby.
  - If you feel like you are the victim of a breach call, don't email, your IT department. They will walk you through all the steps necessary to isolate the potential event/incident.

How to Protect Your Personal Data if Hacked

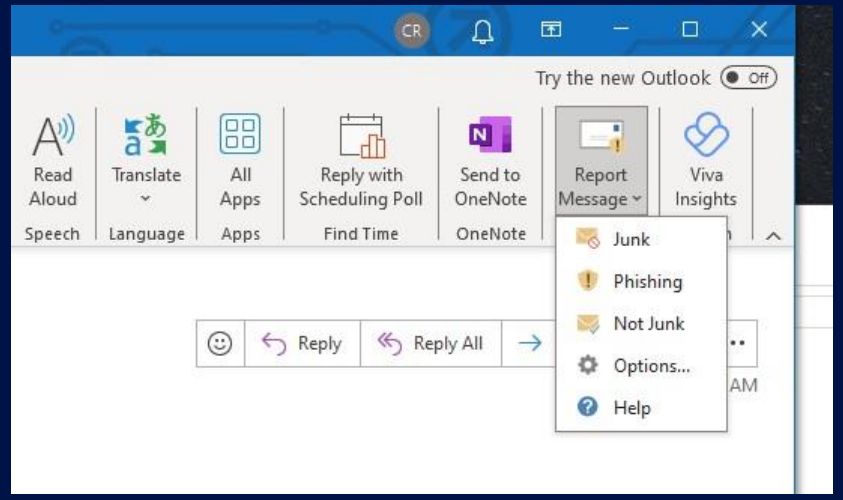
- Change your Passwords. (Bank and Payroll Accounts, Credit Cards, Personal and Work Email Accounts, Online Shopping, Teacher Resources and School Vendor websites, etc.)
  - Changing passwords immediately may prevent hackers before they cause any damage.
  - Make the new passwords tricky, hard to guess and different for each website.
  - Start using a password manager with one long and complex password / passphrase.
- Check all your accounts for unauthorized activity.
  - Identify fraudulent purchases or transactions for dispute.
- Notify your bank and credit card companies.
  - Provide details of any identified fraudulent activity.
  - Inquire about FREE credit monitoring.
- Contact the FBI Internet Crime Complaint Center (https://www.ic3.gov/)
  - You may file a complaint with the IC3 if you believe you have been the victim of an Internet crime or if you want to file on behalf of another person you believe has been such a victim.

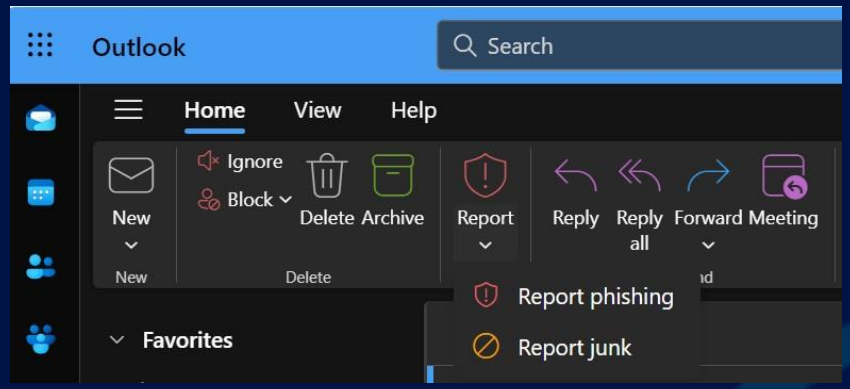
How to Protect Your Personal Data if Hacked

- Tell your friends and family you were hacked.
  - Alert people you communicate with that your email account has been hacked and that the hacker may send strange messages in your name, looking for more victims.
- Continue to monitor your financial and credit accounts.
  - Although your bank may have systems in place to track potentially suspicious activity, only **YOU** know what transactions were authorized.
- Scan your computer for viruses and malware.
  - You'll want to run a security scan of your computer using a leading antivirus program and malware detector, which can help you find and eliminate any programs lurking on your hard drive, waiting to do more damage.
- Notify your school's IT department
  - They should be aware of your breach before you use any device to connect to their network OR if you log into any account using school equipment.

Use the Phishing Button on Email Ribbon

From Outlook Client Version: Click on "Report
Message" and choose one of the options from the Drop
Down menu.





From Outlook Web Version: Click on "Report" and choose either "Report phishing" or "Report junk".

OR

How to Report an Incident

Hempstead Technology Team

516.434.4100

or

Help desk/ticket portal:
A trouble ticket in IncidentIQ

STETSON cybergroup

Thank you!