DIGITAL LITERACY SKILLS

CYBER SECURITY

Module 14

TRAINING PROGRAM FOR VOLUNTEER MANAGERS

CYBER SECURITY

Welcome to Cyber Security! In this Module, we will discuss foundational cybersecurity concepts, such as threat detection and security measures you can take to protect your data and technology.

WHAT IS CYBER SECURITY?

Cyber security is the practice of protecting technological devices and online information from digital threats. Note there are a few different types and methods of cyber security:

- **Network security**

This is protecting your computer's network from any threats. This protects your internet connection, like Wi-Fi, from being hacked or attacked. Ensure your Wi-Fi network is secure by locking it with a password you and other authorised users know.

If you're accessing Wi-Fi outside your home, like at the library or cafe, make sure you use a secure Wi-Fi network. It is not secure if the Wi-Fi doesn't require a password to log in. You can use this for basic internet browsing, but avoid using it for private or sensitive purposes, like logging into a bank account or email.

- **Application security**

These are any measures you take to keep your software and devices safe. Account logins are great examples of this: You use passwords and other features to authorise access to your applications.

WHAT IS CYBER SECURITY?

- **Information security**

This protects your data and keeps it private. You can strengthen your information security by only storing sensitive information in secure, password-protected locations.

- **Operational security**

This is mainly used within organisations. Operational security might ensure that only certain groups or individuals can access or log into online programs or files with important information.

- **Business continuity and disaster recovery**

These should be in-depth plans organisations have in place in the case of a cyber security attack. For example, they might back up or store important information in 2 different secure files or applications in case one gets compromised.

- **End-user education**

Organisations should have policies and tutorials in place to help their members and users know how to use their software, website, or other online resources safely and confidentially.

WHAT IS CYBER SECURITY?

Important Cyber Security Terms to Know:

- **Hacking**: When a cybercriminal or hacker gains unauthorised access to a digital device, network, or software. This is typically done to steal or compromise online data.

- **Phishing**: A way hackers steal your personal information. This is often through emails, social media messages, and text messages that may look authentic but are attempts to steal sensitive information, like bank account number or passwords.

- **Data breach:** When a hacker gains access to a system's information.

- **Firewall**: A defensive cyber security system used to protect devices from hackers.

- **Malware**: Software downloaded that can steal and corrupt information on a computer. It can often hack into a device if you click on a fraudulent link or download an insecure file or application.

- **Virus**: A type of malware that changes or erases information on a computer and then shares it with others.

- **Ransomware**: A type of malware that keeps you from being able to access your computer's files. It takes the data for ransom.

- **Spyware**: Malware that secretly spies on user activity, like logins, passwords, payment information, and more.

CURRENT AND EMERGING CYBERSECURITY THREATS

Ready to upgrade your cyber security? Let's focus on the measures we can take to protect our data and devices.

To protect yourself against any threat, you must know how it attacks. The 2 most common ways your data or devices may be compromised as a user are phishing and personal data breaches. Let's review each of these:

Phishing

Phishing occurs when a cybercriminal poses under a fake identity to obtain your information. They'll reach out via email, social media, or text message.

At work, they might pretend they are your colleague, an important company, or even your manager and request access to sensitive information about your company, like a login, password, or important file.

Personally, they might pose as your friends, family members, or a legitimate organisation reaching out for informationor money.

How to Detect Phishing Scams

So, how can you know if these messages are real or fake?

There are 6 main traits that signify a phishing attack. Even if they only express one of these traits, they can be fraudulent:

1. They're overpromising.

If you receive an email or message saying you've won a prize, contest, or any other free claim that sounds too good to be true, it's almost guaranteed to be a phishing scam.

2. They claim you owe money.

On the flip side, scammers use fear tactics to steal your information. They'll claim that you owe money, your information is compromised, or you're in some type of danger –- unless you give them your payment information, passwords, or other sensitive information. This is almost always a scam, and it often takes place through phone calls.

CURRENT AND EMERGING CYBERSECURITY THREATS

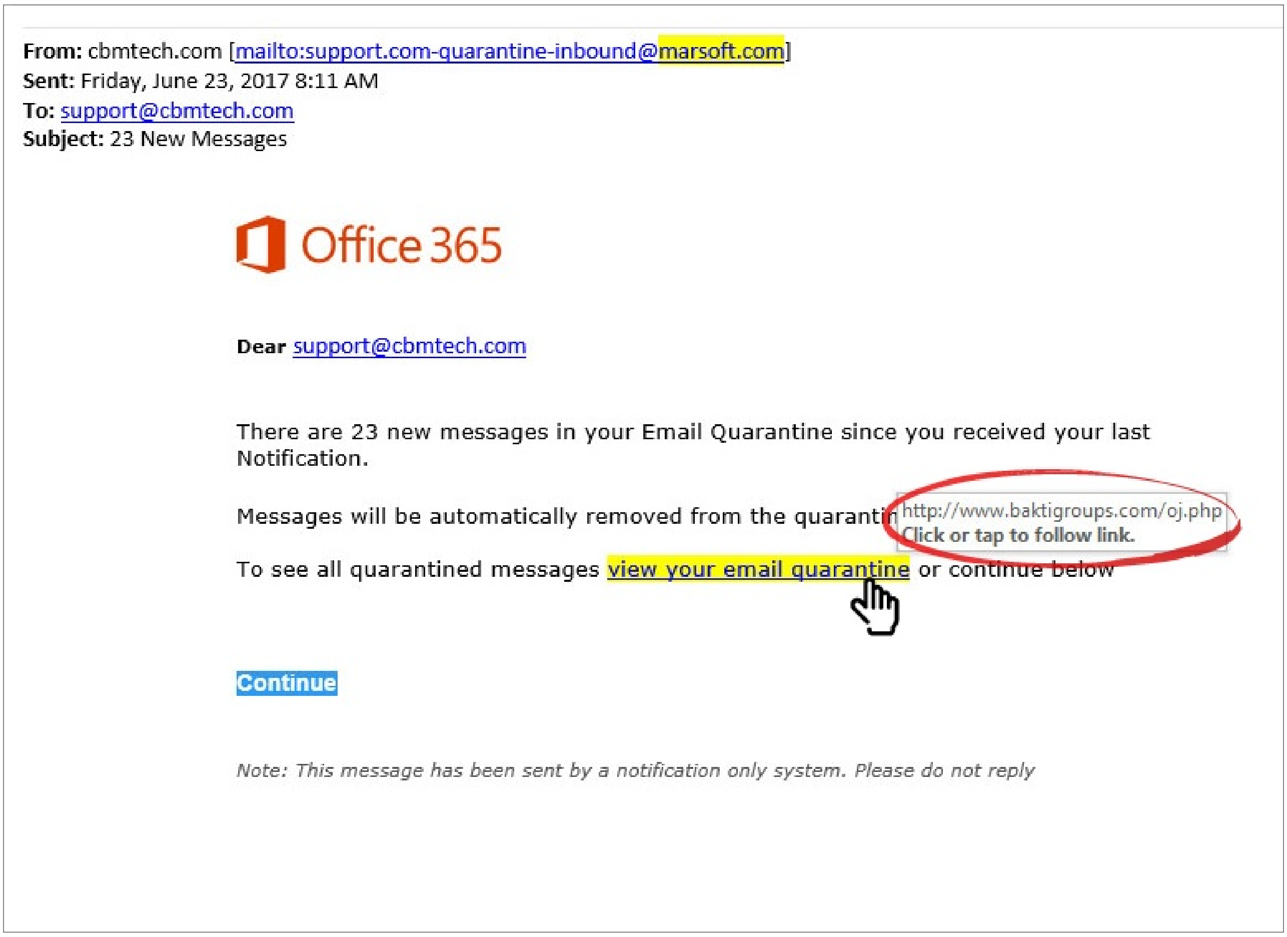
How to Detect Phishing Scams

3. It includes unexpected hyperlinks or attachments.

If a sender includes a link or attachment in an email or message, be wary of clicking on it, even if you know them. This is one of the most common ways to get malware on your device.

If they send a ***link***, hover over it with your mouse and look to see if the URL matches what's written there. If it doesn't match or it's misspelt in any way, do not click on it. If it's a 'bit.ly' or any unfamiliar link, avoid clicking on it. If you know the sender, reach out to them with a phone call to see if it's genuinely them that sent the link or if they've been hacked.

If they send an ***attachment***, right-click over the attachment and open it with your antivirus program. If you're using Gmail, it automatically scans the attachment for you. If it has a virus, you won't be able to download it to your computer.



From: cbmtech.com [mailto:support.com-quarantine-inbound@marsoft.com]
Sent: Friday, June 23, 2017 8:11 AM
To: support@cbmtech.com
Subject: 23 New Messages

Dear support@cbmtech.com

There are 23 new messages in your Email Quarantine since you received your last Notification.

Messages will be automatically removed from the quaranti

http://www.baktigroups.com/oj.php
Click or tap to follow link.

To see all quarantined messages view your email quarantine or continue below

Note: This message has been sent by a notification only system. Please do not reply

CURRENT AND EMERGING CYBERSECURITY THREATS

How to Detect Phishing Scams

4. They're acting as if a response or action is urgent.

If a message consistently tells you to 'act now' or that you only have seconds or minutes to 'receive your deal', it is likely a scam.

5. You don't recognise the sender, or the content is out of character.

If you've never received an email or message from the contact, avoid clicking on or replying to it.

Even if you know the sender, you should avoid clicking on any messages that seem out of character. For example, cryptocurrency scams are prevalent online. If you have a friend or colleague who you know would never message you about cryptocurrency, it's very likely a scam.

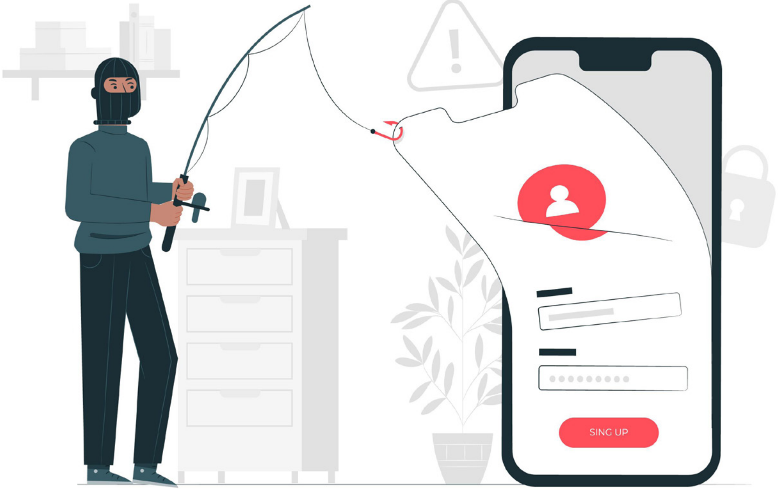
6. The sender and name are inconsistent.

Always compare the email address and sender's name before clicking on, replying, or opening links/attachments. For example, the email might say it's from Olivia Smith. But if you look at the sender's email address, you might find a strange combination of letters/numbers or a misspelt version of the name.

If you're on your phone or social media account, be careful if a sender claims to be a friend but uses a different phone number or social media account.

Recently, scammers have gotten even more sophisticated by simply creating an email address that slightly misspells the name of the person or company they're pretending to be.

For example, a group of hackers used the email address "security@mail.Instagram.com," to send messages to users saying their accounts were compromised. They needed to log back into their account using the link to regain access. The format and style of the email looked very similar to Instagram's actual email -- the only difference is they used a lowercase "L" instead of an "i" for the word "instagram." Their actual email address is "security@mail.instagram.com." Very subtle, yet very dangerous!



CURRENT AND EMERGING CYBERSECURITY THREATS

Personal Data Breaches

Personal data breaches occur when hackers obtain unauthorised access to an organisation's information. Most often, hackers are after the personal data companies have about their customers, including their login, payment information, and other sensitive data.

Even the most reputable companies experience data breaches, including Facebook, Twitter, and Yahoo.

How to Protect Yourself Against Data Breaches

- **Create high-security passwords.**
  Include a combination of uppercase and lowercase letters, numbers, and special characters.

- **Use a different password for every website.**
  Change your password often and ensure they're not predictable. For example, a password using your name or publicly available information (like a birthday or location) can be easily guessed.

- **Stay up-to-date on cybersecurity news.**
  Learn which companies have recently had data breaches.

CURRENT AND EMERGING CYBERSECURITY THREATS

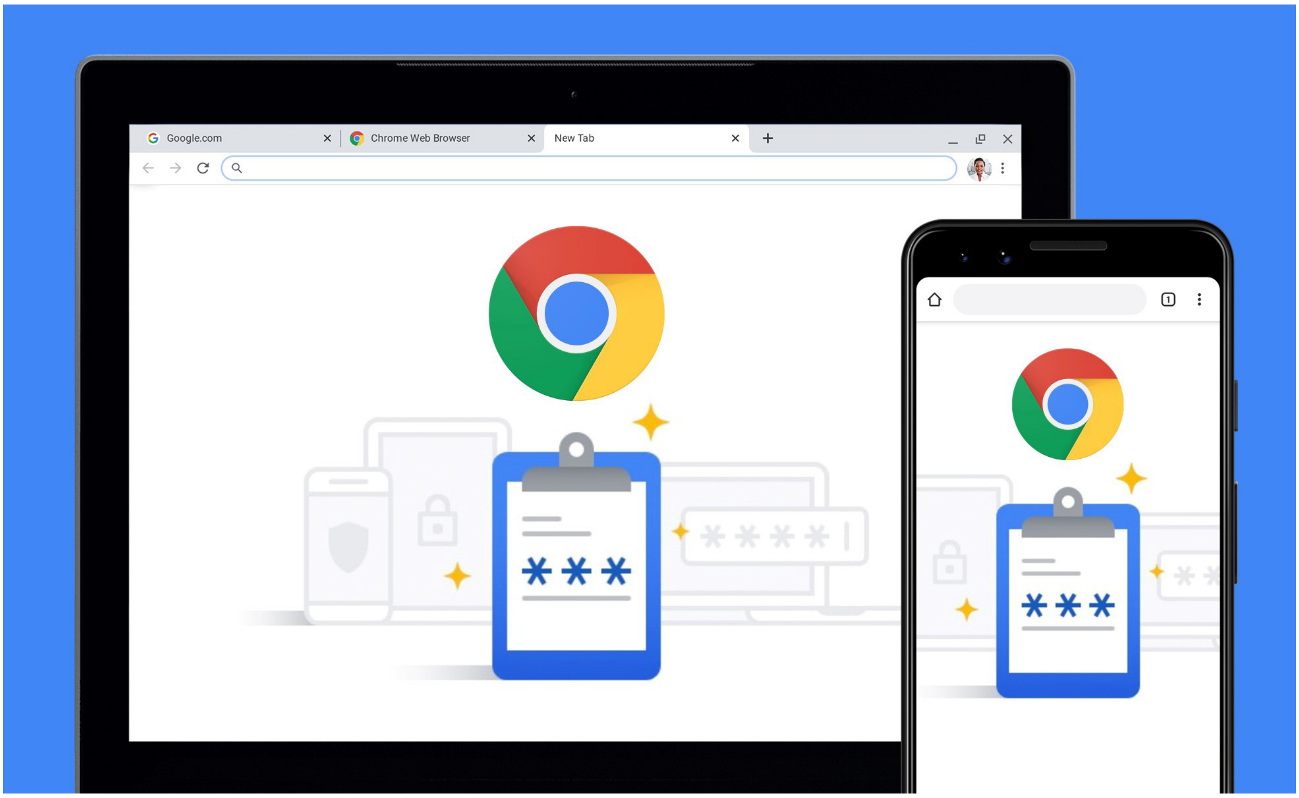
How to Protect Yourself Against Data Breaches

- **Use a secure credit card for online purchases.**
  These are easier to track and cancel if they get hacked.

- **Set up account alerts with your sensitive accounts.**
  For example, you can have your Gmail account send you a message whenever there's an attempt to log into your account.

- **Use 2-factor authentication.**
  Some applications or websites allow you to use this feature to ensure your security. Essentially, you'll need to type in your password and verify it's you logging into your account on a separate device, like your phone or tablet.

- **Use Google's Password Manager.**
  Google's Password Manager allows you to access and manage your passwords in one place. Use their Password Check-up feature to see if any of your passwords have been compromised in a data breach. If so, don't worry –– you can change the password and take check in on your account.



LET’S PRACTICE: CASE STUDIES

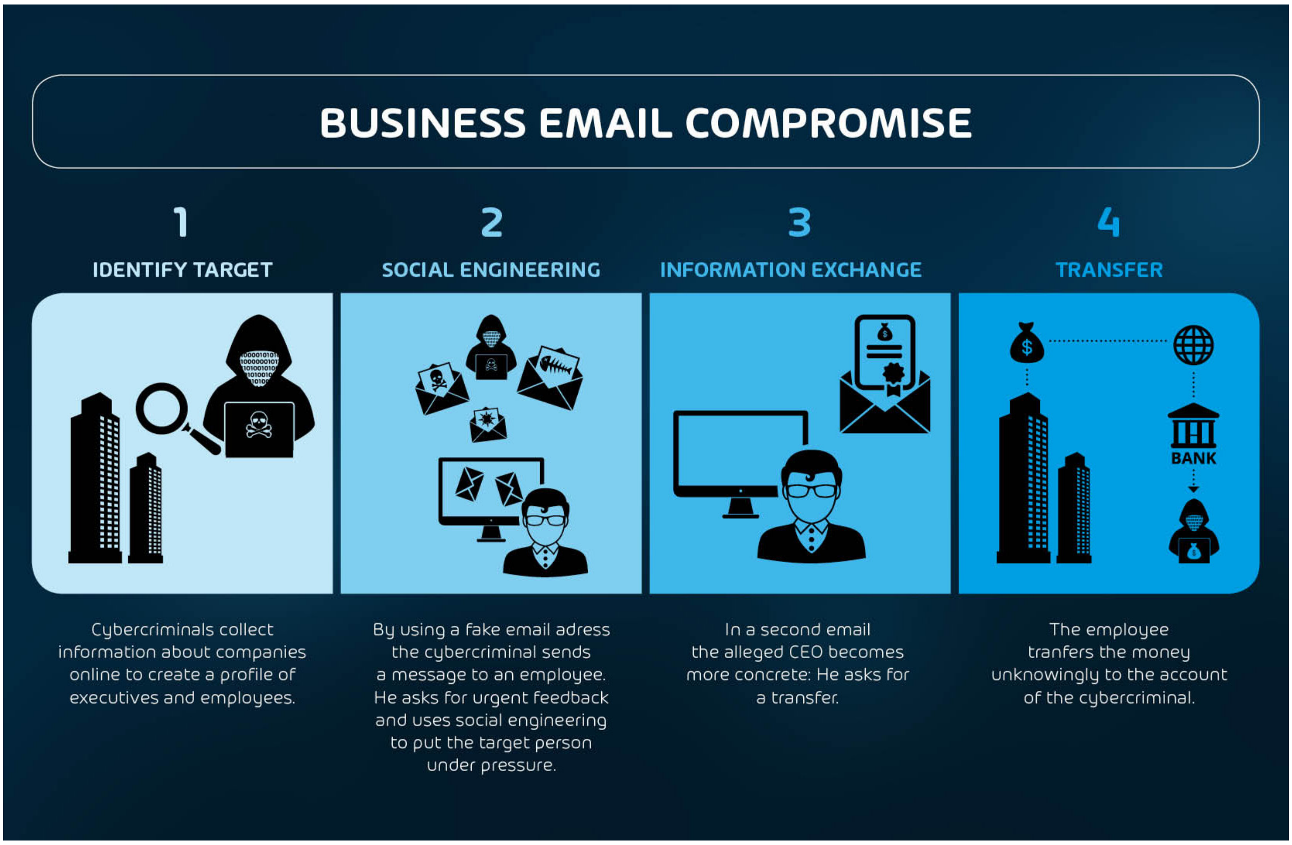
Let’s solidify your learning by putting your cybersecurity knowledge to the test. Follow the scenarios below to see real-life examples of how cyberattacks happen and the key lessons learned from each attack.

Business Email Compromise: Case Study

FACC AG is an aerospace company in Austria. In 2016, phishing scammers pretended to be the company’s CEO and emailed its employees asking to send money for their new project. They lost EUR 24 million.

Lesson learned:

Phishing scammers often target remote employees, pretending to be their superiors. CEOs, managers, or colleagues will never request personal or payment information via email or message. Verify before replying to any suspicious emails at work.



BUSINESS EMAIL COMPROMISE

1 IDENTIFY TARGET

Cybercriminals collect information about companies online to create a profile of executives and employees.

2 SOCIAL ENGINEERING

By using a fake email adress the cybercriminal sends a message to an employee. He asks for urgent feedback and uses social engineering to put the target person under pressure.

3 INFORMATION EXCHANGE

In a second email the alleged CEO becomes more concrete: He asks for a transfer.

4 TRANSFER

The employee tranfers the money unknowingly to the account of the cybercriminal.

LET'S PRACTICE: CASE STUDIES

Ransomware: Case Study

A construction management company experienced a ransomware attack. None of the employees could use their work devices or access their files, leaving 30 employees out of a job for over a week. The hackers holding the data for ransom said they'd only give it back if the company paid them $60,000 in Bitcoin.

The company worked with a cybersecurity agency to recover the data but still had to pay the ransom to restore it.

Lesson learned:

The company had no off-site backups or other ways to access the information they needed without their computers. They were smart to work with a cybersecurity company to restore it, but preventative measures could've helped prevent it.

LET'S PRACTICE: CASE STUDIES

Data Breach: Case Study

Not all data breaches are caused by hackers and scammers. In 2018, a Strathmore College employee accidentally published student records, including protected health and medical conditions. It took a day to get the information down, but during that time, users could access and download this personal information.

Lesson learned:

Cyber security training and understanding are crucial for employees, too. Be careful when dealing with sensitive information at work and at home.

KEY RESOURCES FOR FURTHER INFORMATION

- Top Network Firewalls of 2022
- Top Firewall Software and Hardware
- Australian Cyber Security Centre
- Protect Yourself from Phishing Scams
- Google Password Manager and Checkup