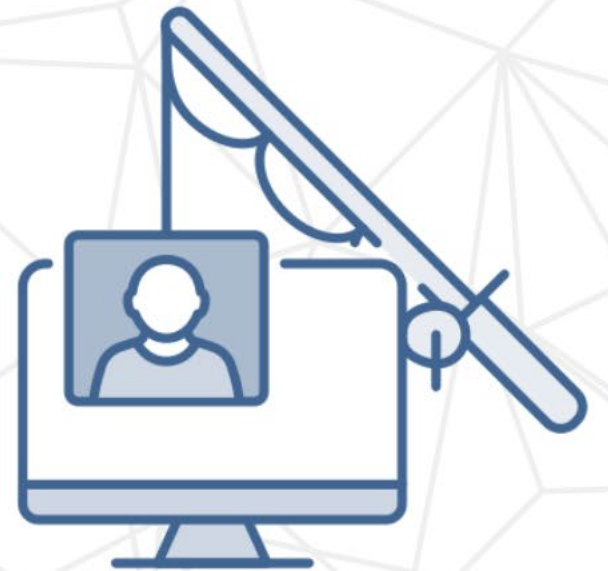# OBJECTIVES

- Protect sensitive data
  - *Bank information, passwords, personal information*

- Avoid being compromised

ATTACKS:
SOCIAL ENGINEERING

- Tricks you into giving sensitive information or doing a malicious action
- Methods use impersonation via phone calls (i.e. call from "IT") and emails
- Be careful, hackers might already have more information than you think

ATTACKS:
PHISHING

- Malicious emails impersonating another entity to harvest information
- Phishing email detection
  - The attacker needs you to interact with the email
    - *Click a link to a login website*
    - *Reply to email with sensitive information such as a password*
- They create a sense of *URGENCY*
  - Target: Fear, Greed, Curiosity or Empathy

AN EXAMPLE OF
PHISHING

To: <undisclosed-recipients>
From: gethacked@publicemailservice.com
Subject: Prize Money Redeem NOW!

Hello,

We have etransfer in the amount $1000000!

This is youre monee.

Click here to deposit

Expir in the next two days.

Thank you,
Mike
RBC

But it's not always that obvious...

BE <u>VIGILANT!</u> 👀

- A Phishing Email can look like it comes from a trustworthy organization or individual
- Focus on 3 parts of the email

Sender Information	Context	Content
WHO is sending this?	WHY are they sending this?	HOW does it make sense?

ATTACKS:
EMAIL SPOOFING

- Pretending to be someone in your organization
  - Sender displays a false sender name from someone you trust or even your own account
- Be suspicious of emails sent to an undisclosed list (exception mailing list or newsletter)
- Be suspicious of organizations with free email services
  - ex: support@publicmailservice.com

EXAMPLE 1 OF

SPOOFING

To: <undisclosed-recipients>
From: payroll@publicemailservice.com
Subject: Payment Deposit

Hello Kim,

We have a Direct Bank Transfer in the amount $1512.30!

This is for the commissions you made in the last two weeks of last month.

Click here to deposit your money

This deposit will expire in the next two days.

Thank you,
Mike
Royal Bank

□ *Should the email sender ask this request?*

□ *Do they already have this information?*

□ *Were you expecting this request?*

□ *Is what they are asking logical?*

□ *Email shows little effort by the sender and asks for personal information*

□ *Grammatical mistakes*

□ *Hover over links*

□ *Be prudent when downloading attachments*

NEVER GIVE OUT YOUR PASSWORD

EXAMPLE 2 OF
SPOOFING

To: Natalie.Forester@aircadetleague.com
From: Pierre Forgues pierrecadets9@publicmailservice.com
Subject: Extl Payroll Account Change

Caution: External email. Be wary of links and attachments.

Hello Natalie,

I have recently changed bank accounts. Please update your payroll records to this banking infomation:

Account: 987654
Institute: 003
Transit: 01503

Thanks,

Pierre Forgues

Ask yourself…

□ *Does it come from my organization?*

□ *Are there external tags?*

□ *Why is the sender using a personal email?*

□ *Are there grammar or spelling mistakes?*

□ *Should I reply to find out more?* **NO**

CALL THE PERSON OR SEND AN EMAIL TO THEIR ORGANIZATION EMAIL

TO CLICK OR NOT TO CLICK?

To: <john@aircadetleague.com>
From: k@aircadetleague.com
Subject: Cybersecurity Training

Hello John,

To check if your current password is on the list of passwords exposed in

data breaches go to the following website:

haveibeenpwned.com/

Regards,
Kim

!!!

https://haveibeenpwned.com/Passwords

✔ *Hover over a link before clicking!*

✔ *Do not click if you are not sure!*

INSPECTING LINKS

www.paypal.com/ca/webapps/mpp/home

Good link! What comes after the first '/' is not important

paypal.com.sales-buy.cn/services

Bad link! What comes before the first '/' is important.
.cn = China not Canada
.sales-buy is not in the real PayPal domain

www.R0YALBANK.com

Bad link! A zero is replacing the O. Search for character substitutions.

CLICK HERE

Click here

CLICK HERE

PHISHING/SPOOFING PASSWORD RESET

To: <tom@aircadetleague.com>
From: execdir@aircadetleage.com
Subject: Password Change Required

Office 365

Hello tom@aircadetleague.com,

Password for tom@aircadetleague.com will expire in 2 days time.

Keep ' current password, Update below:

keep my current password

aircadet.com Service-Support

Microsoft

aircadet.copy.password.cn/keepPassword

- Were you expecting this?
- Hover over the link
- *If you are not sure:*
  - Do not use the link from the email
  - Call
  - If possible, go to the real website

The Trap's Goal

- Will ask you to type in your password to "keep" your current password

PASSWORDS

Passwords are hacked because most people follow patterns

Good Password Practices:

- At least twelve characters long
- Use uppercase and lowercase letters
- Use numbers
- Use symbols
- Multi-factor authentication augments passwords
- Passphrases are a good way to have a password that is longer and easier to remember

GOOD PASSWORDS

Distres3s-plAsma-aplomb

loaF-munition5-eider

BAD PASSWORDS

pa$$word1

cadets2023!

WHAT TO AVOID

✖ A single dictionary word

✖ Writing down your passwords

✖ User IDs, names, locations, birthdays, technical words

✖ Reverse spelling words

✖ Reusing passwords for everything

✖ Sharing your passwords

WHAT TO DO

✔ A combination of random words

✔ Password managers to auto-create and save passwords
Ex. Bitwarden, 1Password

MALWARE
(MALICIOUS SOFTWARE)

Beware of viruses and their diversity:

- *Trojans* – hidden in useful looking programs
- *Web scripting* – infects from webpages
- *Browser Hijacker* – hijacks browser to redirect you to websites
- *Macro virus* – spreads through attachments and infected documents
- *Ransomware* – will encrypt all your files and request a ransom to decrypt
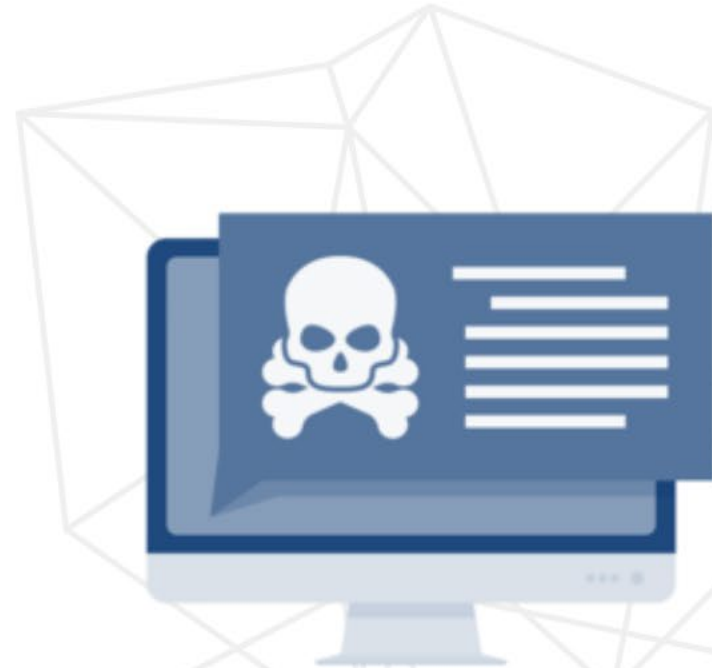
INFECTION METHODS

- *Opening attachments or links from malicious senders*
- *Clicking online ads*
- *Social Media*
  - *e.g. your friend sends you this funny video, CLICK NOW to watch! I saw you in this video!*
- *Unpatched software*
- *Downloading unofficial software or media from websites*
  - *e.g. Downloading pirated movies*

MALWARE IMPACT

- *Erase data*
- *Steal passwords or data*
- *Corrupt files*
- *Spam your contacts*
- *Take over your computer*
- *Encrypts your files*

DO YOU ALREADY HAVE A COMPUTER VIRUS?

- *A lot of pop-up windows*
- *Your homepage is different*
- *Large quantities of emails being sent from your account*
- *Frequent crashes*
- *Slow computer*
- *Unknown programs start when you start your computer*
- *Unusual password changes*

MALWARE PROTECTION

- Backup your important data (prevents ransomware)
- Update your devices and apps, updates can fix vulnerabilities
- Install anti-malware software
  - Warning! Viruses are sometimes disguised as anti-malware software
  - Free anti-malware software such as Windows Defender (Windows) or XProtect (macOS)
    - *Purchase CrowdStrike for more advanced protection*
  - Do not download software that is not from an official or trusted source

PUBLIC WIFI AND HOTSPOTS

- Only connect to WIFI you trust
- Only connect to WIFI and hot spots that are password protected and secure
- Insecure network connectivity: do not connect to open WIFI hotspots (e.g. hotel) unless using a VPN
- Disable auto-connect to WiFi
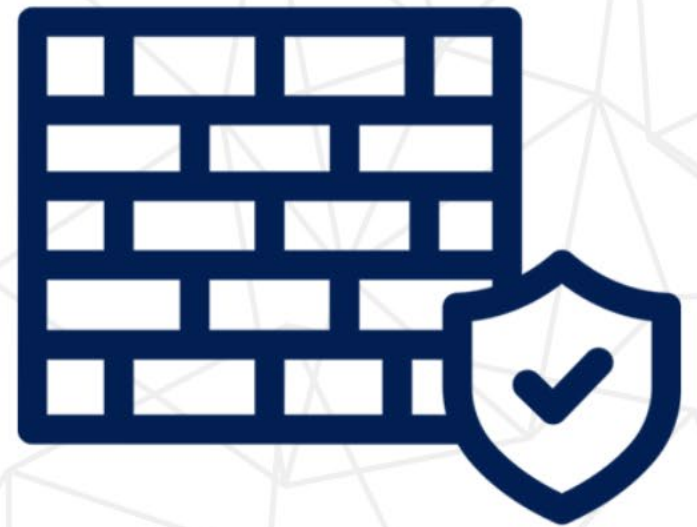- Only use HTTPS websites

FIREWALLS AND VPNS

- **Firewalls**
  - Set your security preferences and decide what can reach your computer
  - Can block certain sites
  - Protect your network from outside networks (internet)
- **VPNs**
  - Allow you to be anonymous and unmonitored on public open hotspots
  - Protect your privacy and can encrypt your data

FILE SHARING

- Do not use your personal account for your organization
- Use secure file sharing cloud services : OneDrive/SharePoint, Google Drive
- Use anti-malware software and install/enable firewall
- Share files to people who are trusted or are from the same organization
- Do not store private information on a non-encrypted USB key in case of loss or theft

Risks

- Installing malicious code
- Exposing sensitive information
- Giving accidental permissions to do more than you want

TRAINING RECAP

- Inspect emails
- Follow good password practices – consider using a password manager
- Inspect a link before clicking it
- Be cautious when downloading or opening attachments
- Download trustworthy software from official sources
- Beware of public WIFI and hotspots
- Go on HTTPS websites
- Consider using a VPN and antivirus application
- Update your devices to latest software
- Make sure your device settings are secure – disable auto connect in your WIFI settings

QUESTIONS?

K@K2ESEC.COM

BACKGROUND AND SUPPLEMENTAL INFORMATION

Windows Owner – Windows Defender

- Real-time protection against spyware, viruses, and other malicious software
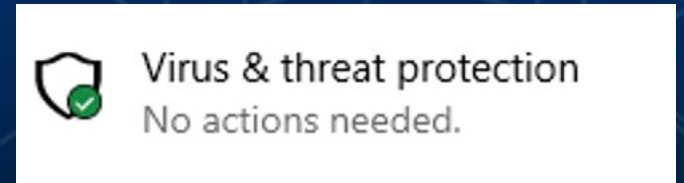
1. Click the start button (Windows button)

2. Windows security
    Green Tick means an antivirus program is present. No action needed

3. Virus and threat protection

4. Virus and threat protection settings

5. Make sure Real-time protection is on

https://docs.microsoft.com/en-us/mem/intune/user-help/turn-on-defender-windows

Mac owners - XProtect

- Macs have a built-in basic antivirus (XProtect)
- Checks applications you run and compares them to a list of known bad malware

- System Preferences > Software Update > Install system data files and security updates (OS X 10.10 or later)

- This will make sure XProtect is updated

https://support.apple.com/en-ca/guide/security/sec469d47bd8/web
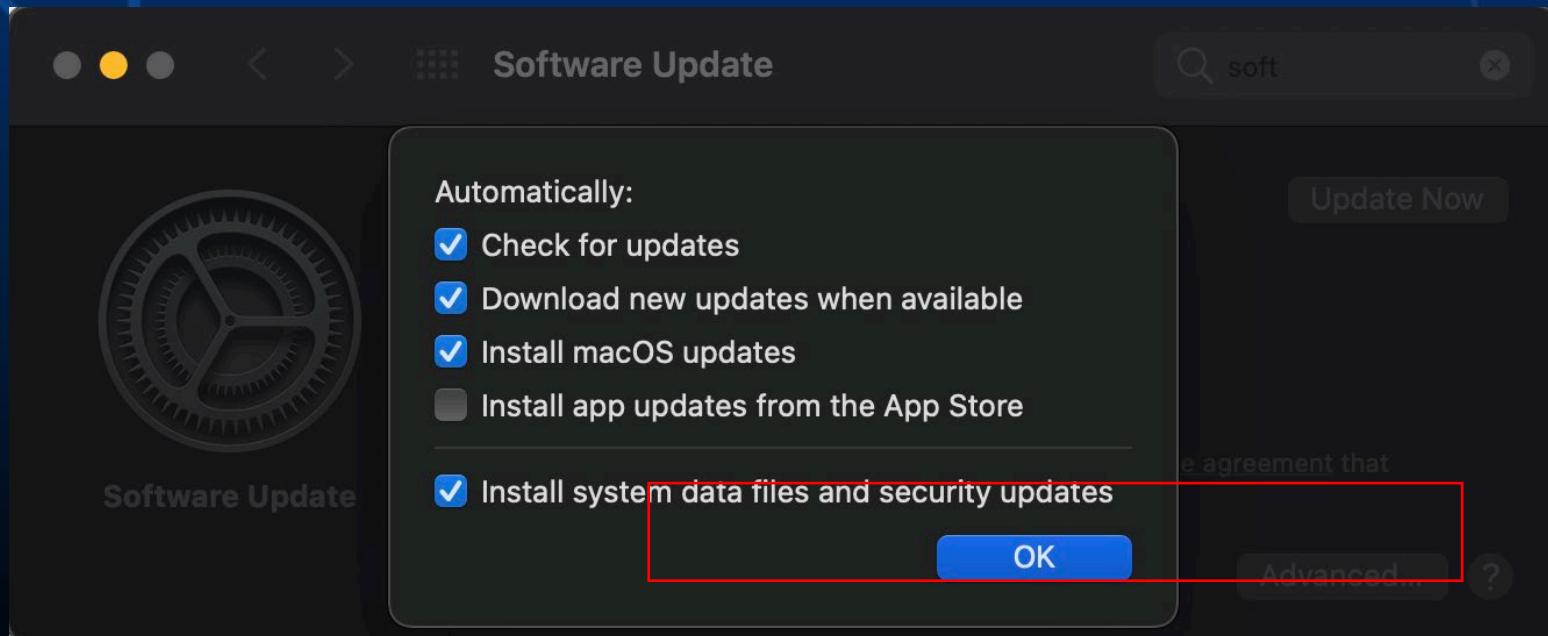
Gmail – Two-Factor Authentication

1. Open https://myaccount.google.com/

2. Navigation panel > Security

3. Under "Signing in to Google" > 2-Step Verification > Get started

4. Follow steps on screen

https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DAndroid

Microsoft – Two-factor authentication

1. Go to https://account.microsoft.com/security

2. Sign in

3. Select "More security options"

4. Two-Step Verification > **Set up two-step verification**

5. Follow the instructions

https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4

How to set up two-factor authentication for Google Suites

https://support.google.com/a/answer/9176657?hl=en&ref_topic=2759193

1. Sign in> Google Admin Console with admin account> Security> 2-Step Verification.
    a) Allow users to turn on 2-Step verification
    b) Select Enforcement off (this will lock out users without 2FA)
2. Tell users to enroll with instructions: https://support.google.com/accounts/answer/185839
3. Optionally Select Enforcement but make sure everyone is enrolled

How to set up two-factor authentication in Microsoft Office Suite

- Admin must enable MFA > Turn on Modern authentication for your organization

Check the following link:

https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?redirectSourcePath=%252fen-us%252foffice%252f8f0454b2-f51a-4d9c-bcde-2c48e41621c6&view=o365-worldwide

- User MFA set up:

1. Sign in like you normally would

2. You will be notified that more information is needed > Click Next

3. Set up the default free Microsoft Authenticator app on your mobile device

https://support.microsoft.com/en-us/office/set-up-your-microsoft-365-sign-in-for-multi-factor-authentication-ace1d096-61e5-449b-a875-58eb3d74de14?ui=en-US&rs=en-US&ad=US

References

[1] A. Grace, "What Is A Computer Virus?" https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

[2] Crystal Bedell, P. Loshin, and K. Hanna, "What is a computer worm and how does it work?," *SearchSecurity*. https://searchsecurity.techtarget.com/definition/worm.

[3] ENOUGH IS ENOUGH, "A Guide to Public Wifi Security Risks & How to Use it Safely," *Internet Safety 101*. https://internetsafety101.org/publicwifisafety.

[4] United States Government, "Risks of File-Sharing Technology | CISA," Cybersecurity and Infrastructure, 2010. https://us-cert.cisa.gov/ncas/tips/ST05-007 (accessed Jul. 26, 2021).