



# CYBERSECURITY TRAINING

K2E Security

# SECURITY AWARENESS

Why be aware?

- Protect sensitive data (bank information, work accounts, personal information)
- Protect the privacy of everyone
- Protect your friends and coworkers

# PROTECT YOUR INFORMATION

- Social Engineering
  - *tricks you into giving information or doing a malicious action*

*Many forms:*

- *Impersonation*
- *Phone calls (call from “IT”)*
- *Emails (Phishing)*

*Be careful, hackers might already have more information than you think*



# PHISHING

- Malicious emails
- HOW TO RECOGNIZE A PHISHING EMAIL
  - *They need you to interact with the email!*
    - Download a file
    - Click a link
    - Reply with sensitive information
  - *They create a sense of **URGENCY***
    - Target: Fear, Greed, Curiosity or Empathy



# Phishing Email Example

**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.

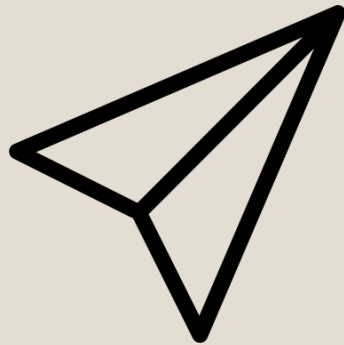
Thank you,  
Mike  
RBC

But it's not always that obvious...

# BE VIGILANT 🙄

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

Sender information



WHO is sending this?

Context



WHY are they sending this?

Content



HOW does it make sense?

# EMAIL SPOOFING

- The Fake “From”
  - Sender displays a false sender name from someone you trust or even your own account
  - This can get past email filters
- 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](mailto:support@publicmailservice.com)

**To:** <undisclosed-recipients>

**From:** ~~gethacked@publicma~~

**Subject:** Prize Money Redeem NOW!

---



execdir@aircadetleage.com

# WHAT TO CHECK?

## Ask Yourself

- ☐ Would the email sender ask this?
- ☐ Do they already have this information?
- ☐ Were you expecting this request?
- ☐ Is what they are asking logical?

## Be Suspicious of

- ☐ Offers that require little effort and ask for personal information
- ☐ General greetings and messages
- ☐ Grammatical mistakes
- ☐ LINKS and ATTACHMENTS

NEVER GIVE OUT YOUR PASSWORD

**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



# EXAMPLE

## Ask Yourself

- Does it come from my organization ?
- Is there a reason why the director wants to give gifts? What's the context? Why are they using his personal email?
- Are there grammar mistakes?
- Should I reply to find out more? NO

**To:** Natalie Forester <Natalie@equispheres.com>  
**From:** Air Cadet Director <pres00208820@wp.pl>  
**Subject:** [External] Quick Task

**WARNING:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Natalie,

Are you available to run an errand? I'm planning to surprise some of the staff with gifts. your confidentiality will be appreciated. I need you to get a purchase done. Email me once you get this.

Regards,

Air Cadet Director

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/](https://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](http://www.paypal.com/ca/webapps/mpp/home)



**Good link!** What comes after the first ‘ / ’ is not important

[paypal.com/sales-buy.cn/services](http://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](http://www.R0YALBANK.com)



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



# PASSWORD RESET EMAILS

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



Hello [tom@aircadetleague.com](mailto:tom@aircadetleague.com),

Password for [tom@aircadetleague.com](mailto:tom@aircadetleague.com) will expire in 2 days time.


Keep ' current password, Update below:

**keep my current password**



aircadet.com Service-Support



 [aircadet.copy.password.cn/keepPassword](http://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 Purpose

- Will ask you to type in your password to “reset” or “keep” your current password



# WHAT TO DO WHEN YOU ARE NOT SURE?

- Send an email, message, phone call, to the person you think sent the email (do not reply directly to the email)
- Friend accounts can be compromised, always analyze links and ask directly if unsure
- Do not open any attachments from questionable sources
- Do not pass along chain letters
- Ask for help!

# 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
- ☐ 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

cadet2

## WHAT TO AVOID



A single dictionary word



Writing down your password



User Ids, names, locations, birthdays, technical words



Reverse spelling words



Same password for everything



Sharing your password



## WHAT TO DO

Combinations of random words



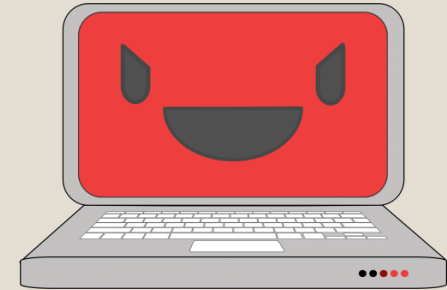
Password managers to auto-create and save passwords  
Ex: Lastpass – password storing  
1Password



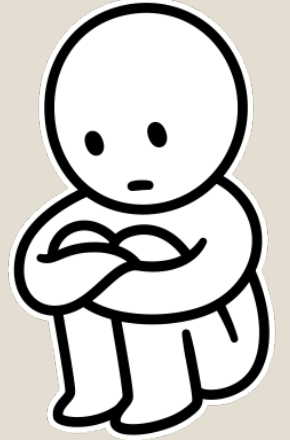
# MALICIOUS SOFTWARE

---

- 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*
  - **Direct action virus** – *when you execute an infected file*
  - **Macro virus** – *spreads through attachments and infected documents*



# Common Ways to Get a Virus



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

**Download Now!**

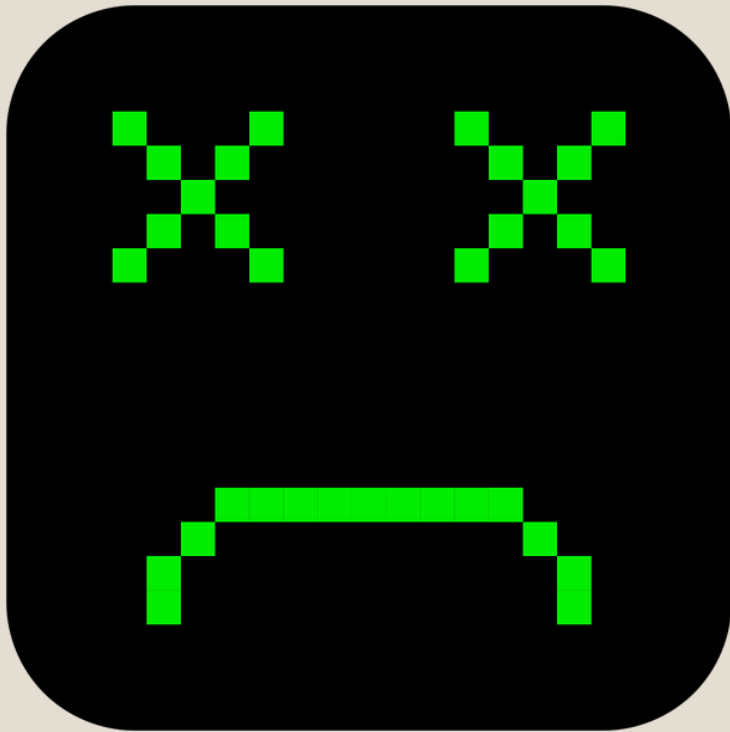


# What a virus can do?

- Erase data
- Steal passwords or data
- Corrupt files
- Spam your contacts
- Take over your computer
- Ransomware – encrypts your files



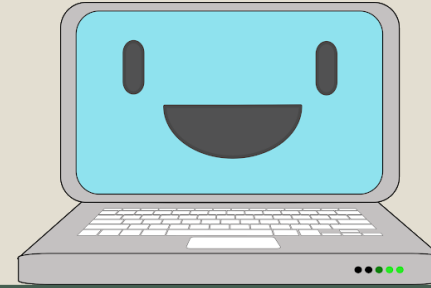
# Do you already have a computer virus?



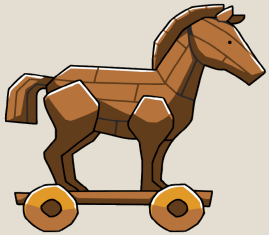
- A lot of pop-up windows
- Your homepage is different
- Large quantities of emails being sent from your account
- Frequent crashes
- Slow computer
- Unknown programs start when you start your computer
- Unusual password changes

# PROTECT YOURSELF

---



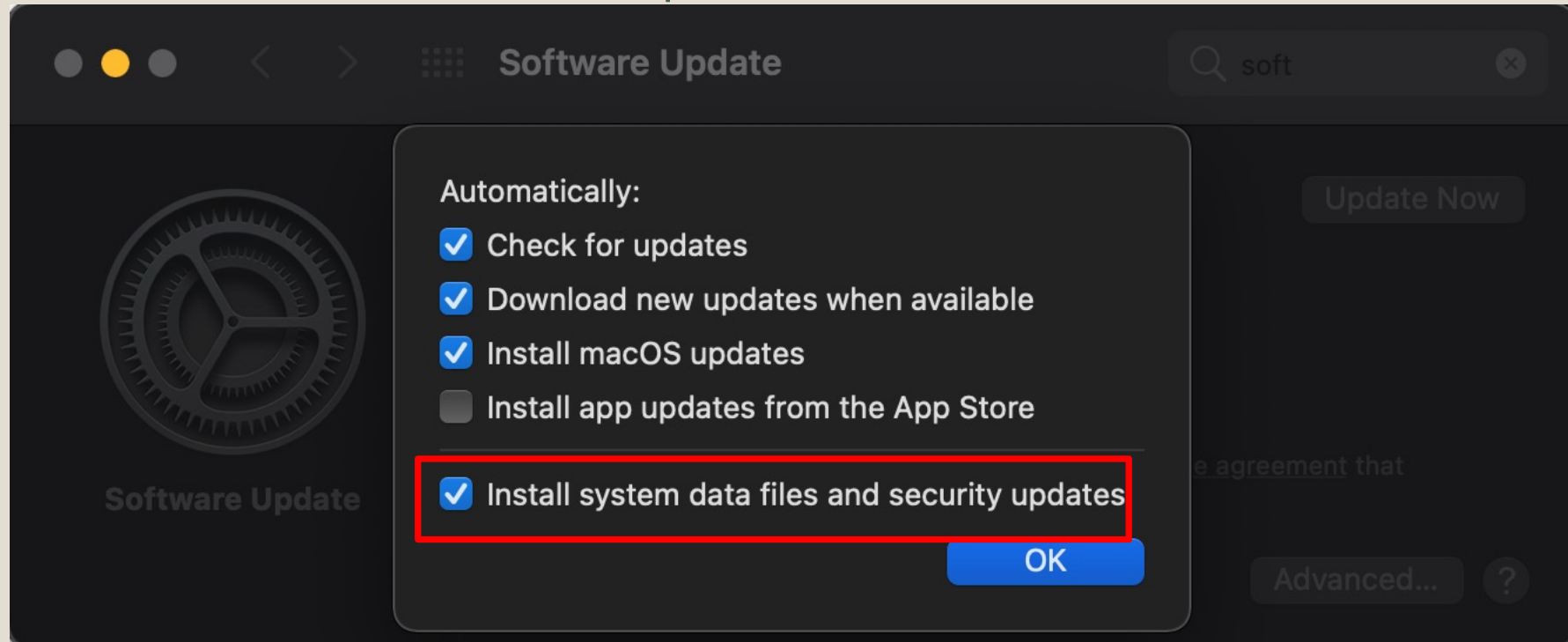
- Backup your important data (prevents ransomware)
- Update your devices and apps, updates can fix vulnerabilities
- Antivirus software



- Warning! Viruses are sometimes disguised as antivirus software (trojan programs)
- Enable Free Antivirus Software: Windows Defender
- Purchase an Antivirus programs such as CrowdStrike for more advanced protection
- Do not download software that is not from an official source

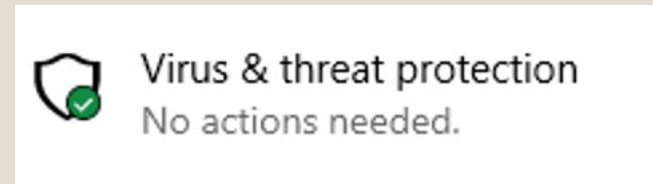
# Mac owners - XProtect

- 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



# 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>

# Public WIFI and Hotspots

---

## Network Worm Viruses

- 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)
- Worms require no user action to spread (through Networks)
  - Find out more:  
<https://youtu.be/oyUsZu6ygq8>

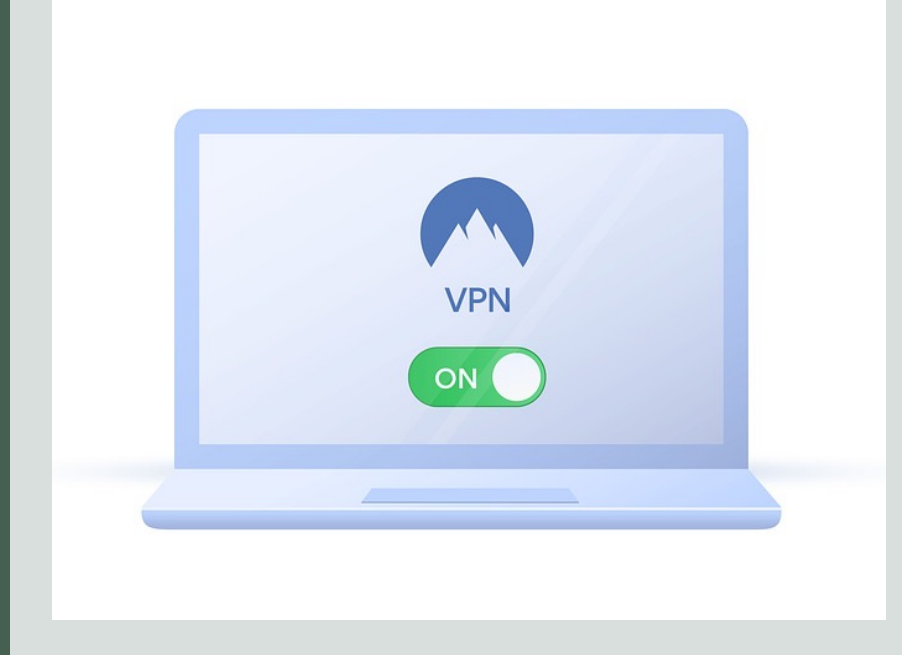






# Network Risks

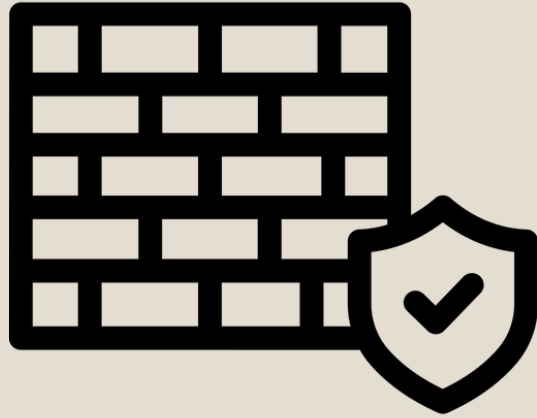
- Mirror Networks: placed near shops to imitate real WIFI networks to steal your information
- Packet analyzers
- Man-in-the-middle attack
- Worms



# Protecting personal information

- Disable auto connect + file sharing
- Only use HTTPS connections
- Use a VPN if possible – provides data encryption

# Firewalls and VPNs



## ■ Firewall

- *Set your security preferences and decide what can reach your computer*
- *Can block certain sites*
- *Protect your network from outside networks (internet)*

## ■ VPN

- *Allow you to be anonymous and unmonitored*
- *Protect your privacy and can encrypt your data*



# Secure Mobile Devices

## ■ How to disable auto-connect?

– *For iPhone:*

*Settings > Wi-Fi > Ask to Join Networks*

*Settings > Wi-Fi > Auto-Join Hotspots >  
Ask to Join*

*In general: Settings > Manage Wi-Fi settings*



# File Sharing

---

- Do not use your personal account for your organization
- Use secure file sharing cloud services : OneDrive/SharePoint, Google Drive
- Use antivirus 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

- Files shared through P2P applications (ex: pirated music) can lead to fines or other legal action
- Installing malicious code
- Exposing sensitive information
- Giving accidental permissions to do more than you want

# 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

A dark green L-shaped graphic element is located in the upper left quadrant of the right half of the image. It consists of a thick vertical bar and a thick horizontal bar meeting at a right angle.

QUESTIONS ?

*k@k2esec.com*



# BACKGROUND INFO



# 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](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).