AC | Information Security and Privacy Office

Cybersecurity Awareness Month 2024

EMPOWERING DIGITAL GUARDIANS:

Defend Against Phishing, Ransomware, and Data Breaches

Learners webinar

October 4th, 2024

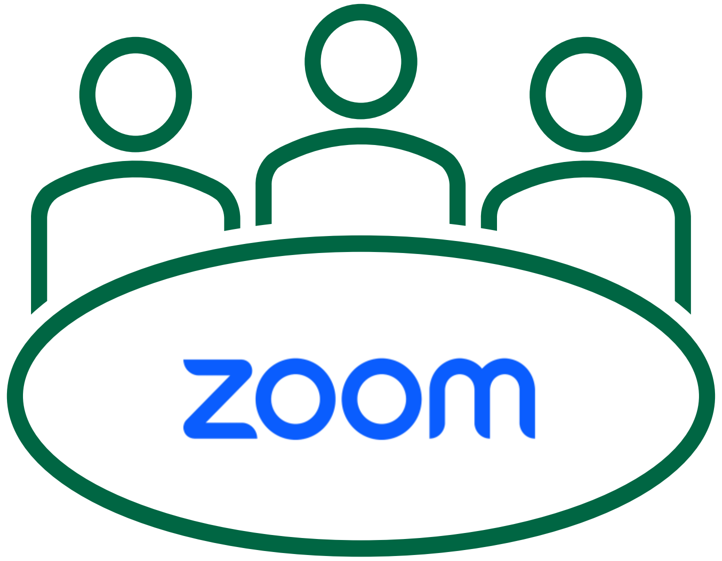
Sponsored by:

CISCO Partner

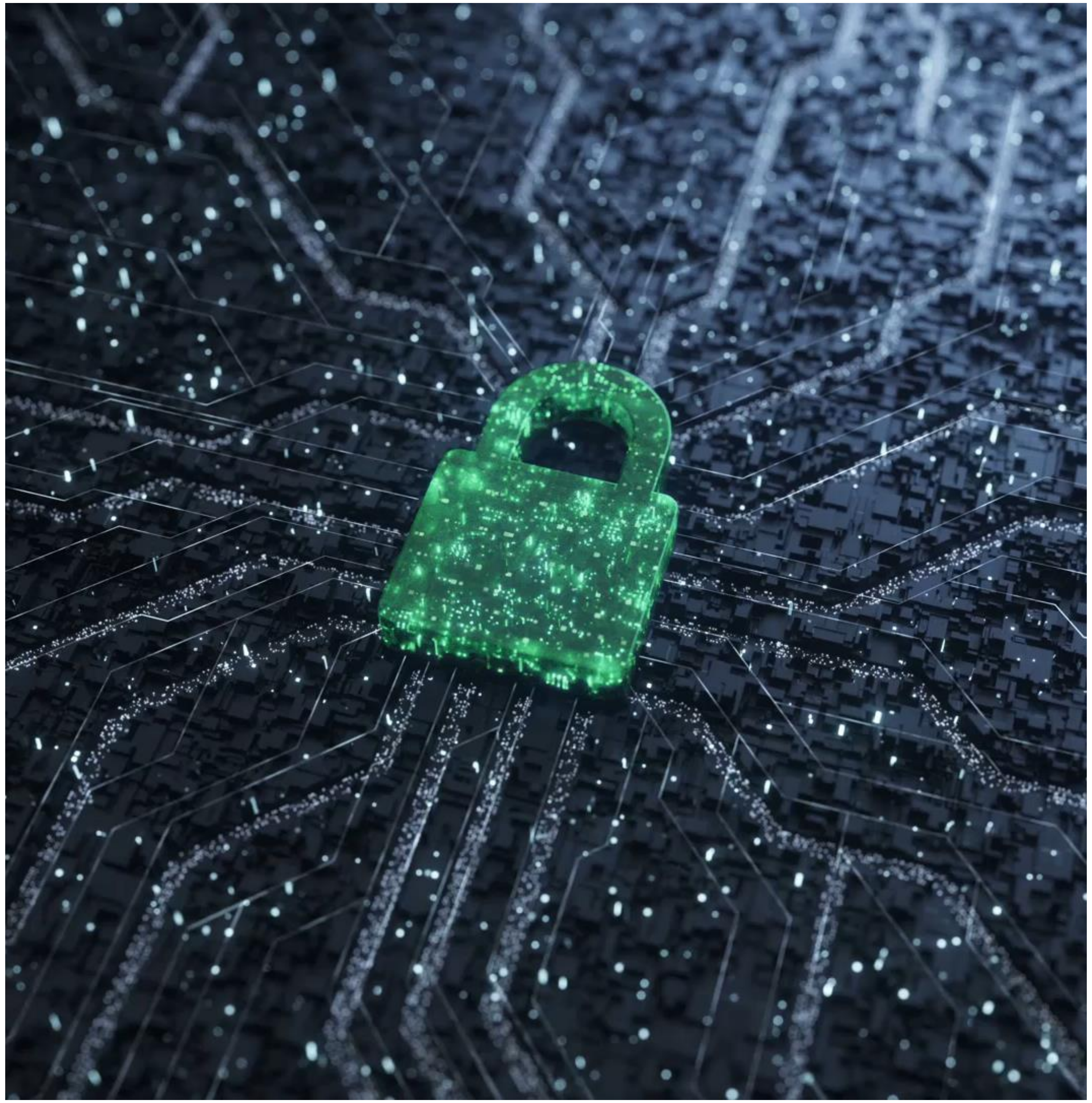
CDW

Webinar Guidance

- Q&A session at the end of the presentation:
  - Use the “Raise Hand” feature to speak or ask a question verbally.
  - Post your questions in the Q&A section.
- This Information session will be recorded and shared with the College Community for future reference



ALGONQUIN
COLLEGE



Agenda

- Who are we?
- What are the most common cyber-threats and how to defend against them?
- Cyber Hygiene: Everyday Practices for Staying Safe Online
- Cybersecurity resources
- Closing Remarks

Who Are We?

Where are we?

The Information Security & Privacy (IS&P) is a dedicated team within the Information Technology Services (ITS) Department at Algonquin College located in the C Building – DARE District in the Ottawa Campus.

What is our Mission?

- To identify, assess, and manage information security and privacy risks to protect the College's digital assets and personal information.

Information Security Unit

- **Information Security Assessments:** Evaluating the security posture of our digital environment.
- **Information Security hardening & maturity:** Securing the College's assets and enhancing practice maturity.
- **Developing policies & compliance:** policies**,** directives, standards, and guidelines to ensure the security of the College's digital assets.
- **Incident Detection and Response:** Identifying and responding to cyber security incidents.
- **Awareness Training Program:** Educating the College community on cyber security best practices.

Privacy Office

- **Support the College** in collecting, using, and disclosing personal information, ensuring compliance with laws and regulations
- **Liaise** with Federal and Provincial Privacy regulators.
- **Advisories on Privacy:** Guidance on privacy-related questions.
- **Promoting a Culture of Privacy:** Encouraging data privacy best practices.
- **Data Breach Response Support**: Assisting in a data breach.
- **Legal and Regulatory Updates:** Keeping the College informed about relevant laws and access requests.
- **Awareness Training Program:** Educating the College community on best practices for privacy.

Information Security and Data Privacy is everybody's business

A Comprehensive Approach

To

Phishing Awareness and Defense

By: Arsalan Parsaei

Cyber Security Program Coordinator

School of Advanced Technology
Algonquin College

Fall 2024

Agenda:

WHAT IS PHISHING?

PHISHING TECHNIQUES

Building Phishing Awareness

Defense Strategy

Phishing Detection & Response

Implementing Best Practices

UNDERSTANDING PHISHING TECHNIQUES

- Phishing attacks come in various forms, including:
  - Email
  - Spear Phishing
  - Smishing (SMS phishing)
  - Vishing (Voice phishing)
  - Clone phishing

IMPACT OF PHISHING ATTACKS

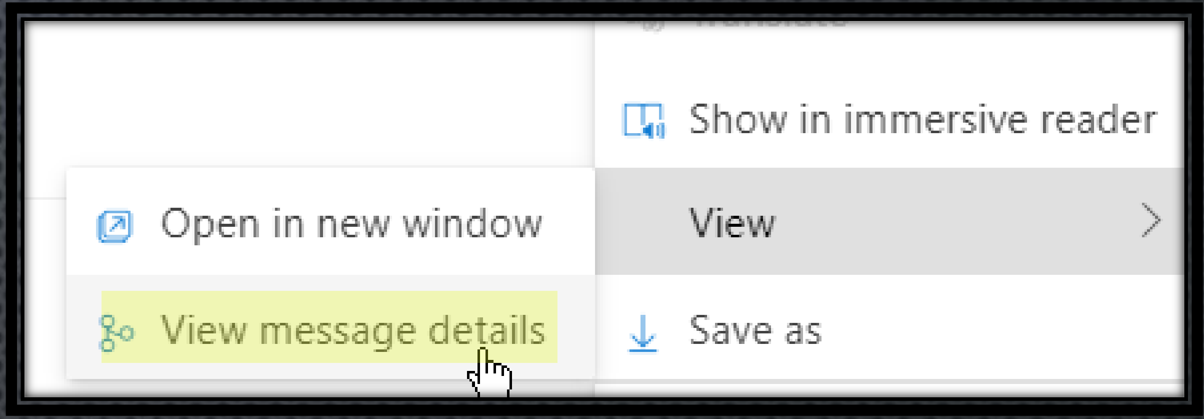
- FINANCIAL LOSSES
- DATA BREACHES
- REPUTATIONAL DAMAGE

BUILDING PHISHING AWARENESS

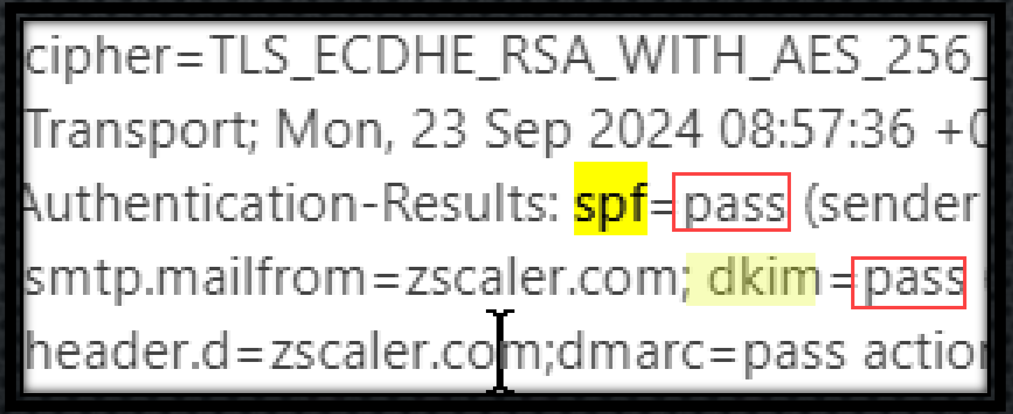
Educating employees about phishing threats is crucial.

A culture of **awareness** can significantly reduce the risk

Phishing Detection & Response (Resources)



- Identify & Detect:
  - https://toolbar.netcraft.com
  - http://www.phishtank.com
- Contain, gather more info, header analyze (SPF , DKIM)
  - https://mxtoolbox.com/EmailHeaders.aspx
  - https://www.ip2location.com/free/email-tracer
  - https://centralops.net/co/EmailDossier.aspx
- Eradicate:
  - Report Phishing using mail client service, delete the email, same process for Gmail & Yahoo & Hotmail



```
cipher=TLS_ECDHE_RSA_WITH_AES_256_
Transport; Mon, 23 Sep 2024 08:57:36 +
Authentication-Results: spf=pass (sender
smtp.mailfrom=zscaler.com; dkim=pass
header.d=zscaler.com;dmarc=pass actio
```

IMPLEMENTING DEFENSE STRATEGIES, BEST PRACTICES

- Organizations should adopt a multi-layered approach to defense against phishing.

This includes using :

Employee Training
Regular phishing awareness training

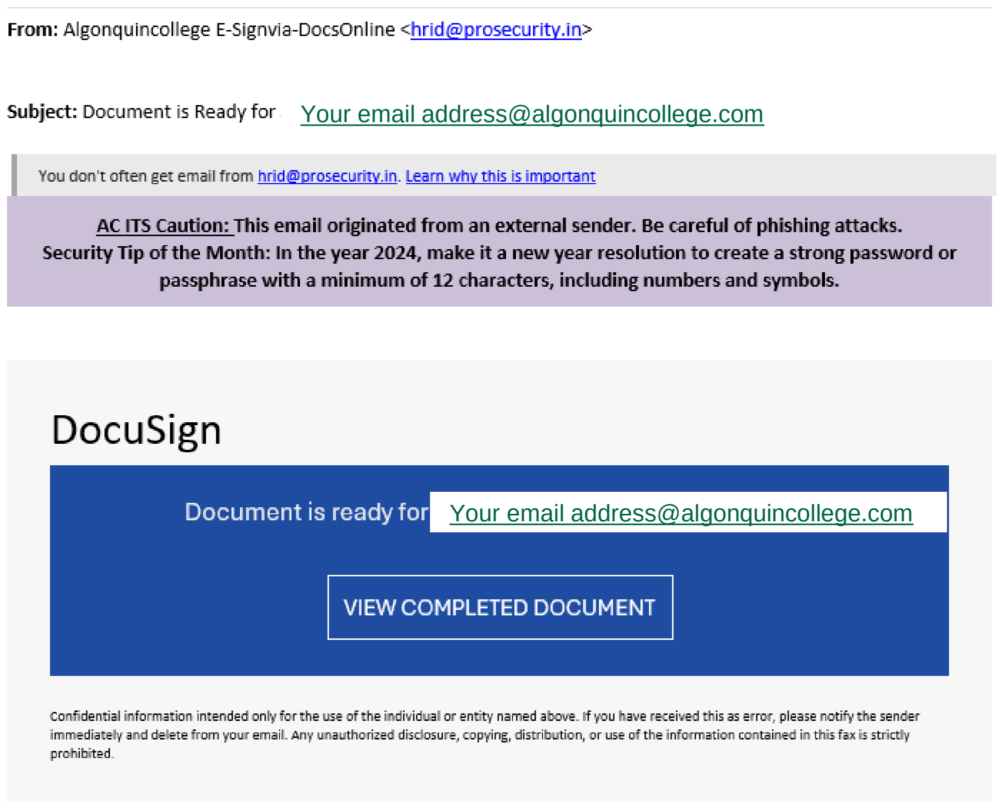
Technical Defenses:
MFA
Email filtering and anti-phishing tools
Auditing & continues monitoring
Using secure emailing system (https://rmail.com/apps/rmail-online

THANK YOU

Common Cyber-Threats

Defending Against Phishing - Examples

1



From: Algonquincollege E-Signvia-DocsOnline <hrid@prosecurity.in>

Subject: Document is Ready for Your email address@algonquincollege.com

You don't often get email from hrid@prosecurity.in. Learn why this is important

AC ITS Caution: This email originated from an external sender. Be careful of phishing attacks.
Security Tip of the Month: In the year 2024, make it a new year resolution to create a strong password or passphrase with a minimum of 12 characters, including numbers and symbols.

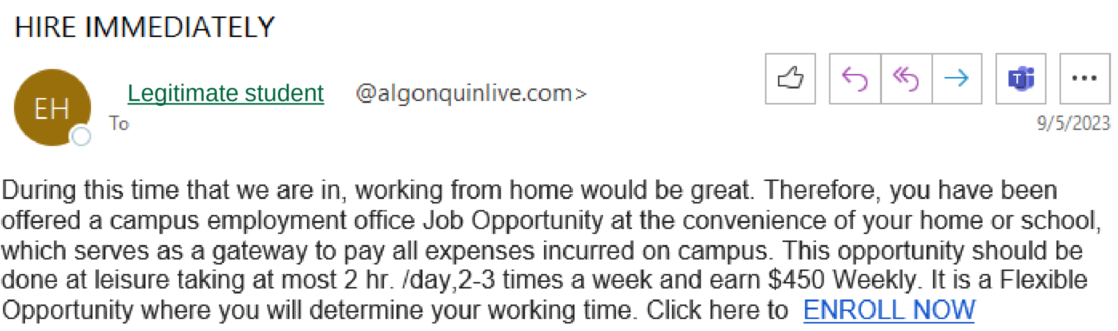
DocuSign

Document is ready for Your email address@algonquincollege.com

VIEW COMPLETED DOCUMENT

Confidential information intended only for the use of the individual or entity named above. If you have received this as error, please notify the sender immediately and delete from your email. Any unauthorized disclosure, copying, distribution, or use of the information contained in this fax is strictly prohibited.

2

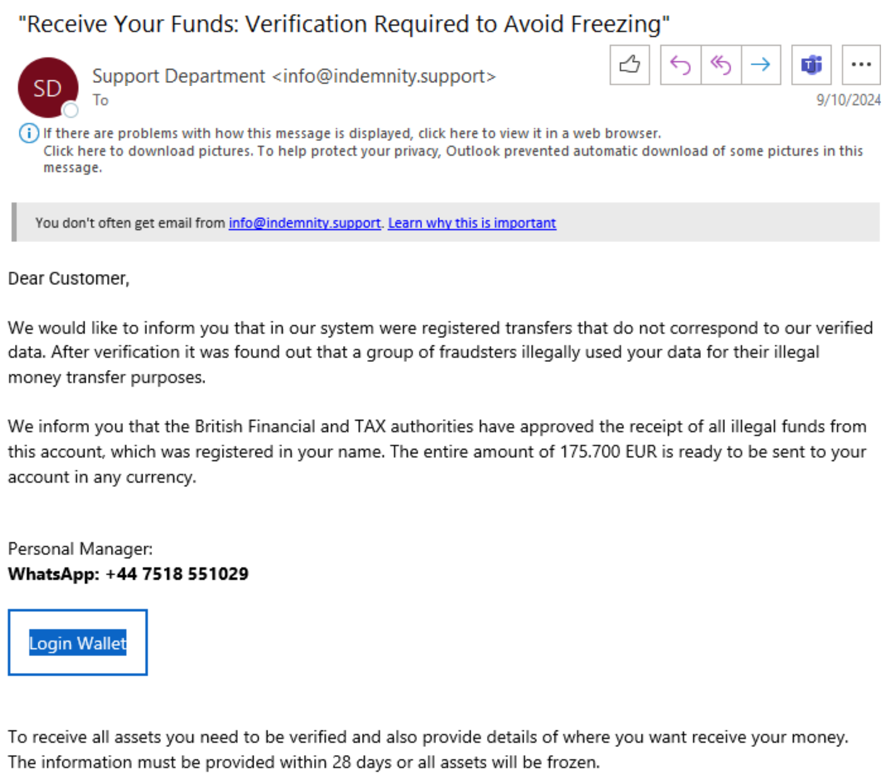


HIRE IMMEDIATELY

EH Legitimate student @algonquinlive.com>
To
9/5/2023

During this time that we are in, working from home would be great. Therefore, you have been offered a campus employment office Job Opportunity at the convenience of your home or school, which serves as a gateway to pay all expenses incurred on campus. This opportunity should be done at leisure taking at most 2 hr. /day,2-3 times a week and earn $450 Weekly. It is a Flexible Opportunity where you will determine your working time. Click here to ENROLL NOW

3



"Receive Your Funds: Verification Required to Avoid Freezing"

SD Support Department <info@indemnity.support>
To
9/10/2024

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

You don't often get email from info@indemnity.support. Learn why this is important

Dear Customer,

We would like to inform you that in our system were registered transfers that do not correspond to our verified data. After verification it was found out that a group of fraudsters illegally used your data for their illegal money transfer purposes.

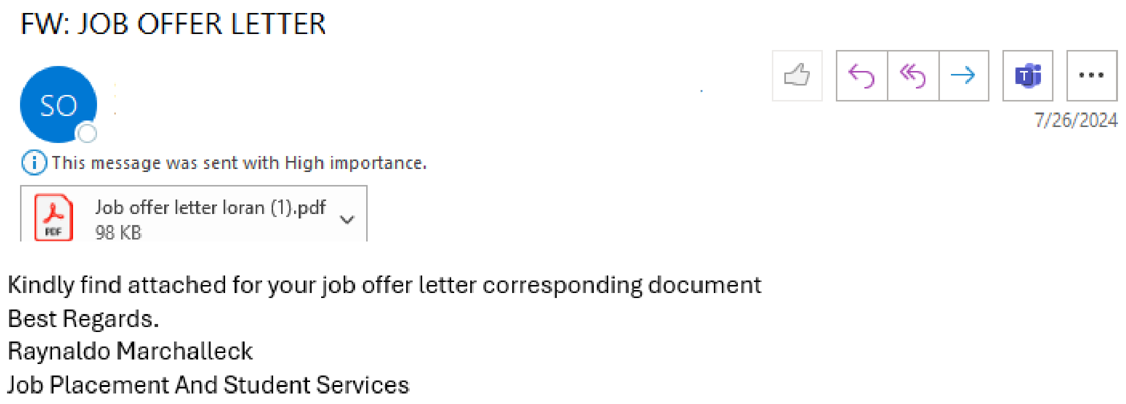
We inform you that the British Financial and TAX authorities have approved the receipt of all illegal funds from this account, which was registered in your name. The entire amount of 175.700 EUR is ready to be sent to your account in any currency.

Personal Manager:
WhatsApp: **+44 7518 551029**

Login Wallet

To receive all assets you need to be verified and also provide details of where you want receive your money. The information must be provided within 28 days or all assets will be frozen.

4



FW: JOB OFFER LETTER

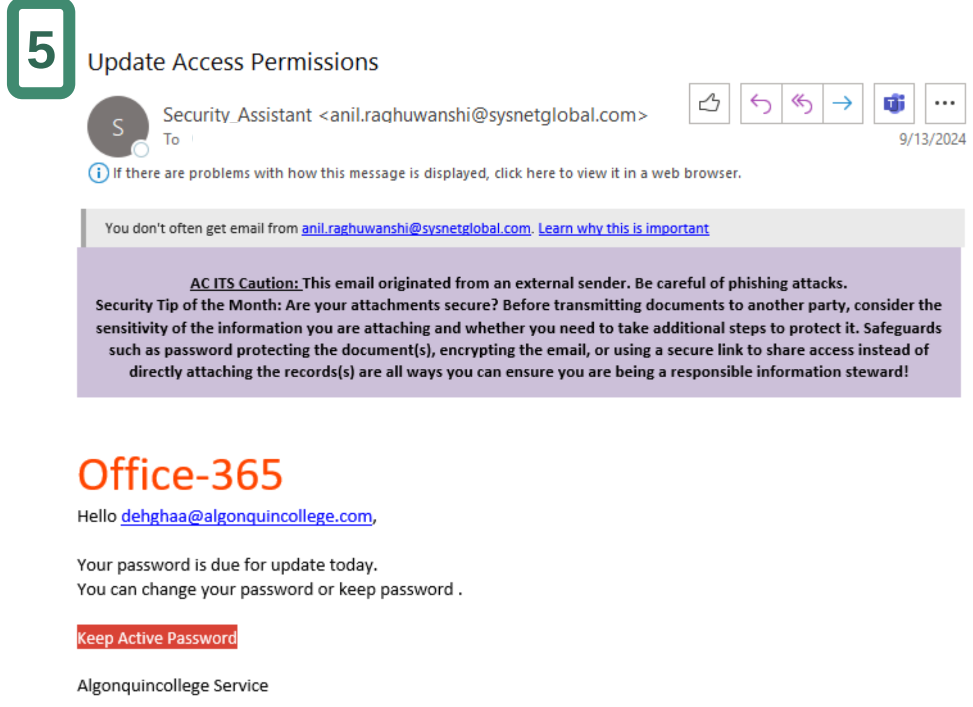
SO
7/26/2024

This message was sent with High importance.

Job offer letter loran (1).pdf
98 KB

Kindly find attached for your job offer letter corresponding document
Best Regards.
Raynaldo Marchalleck
Job Placement And Student Services

5



Update Access Permissions

S Security_Assistant <anil.raghuwanshi@sysnetglobal.com>
To
9/13/2024

If there are problems with how this message is displayed, click here to view it in a web browser.

You don't often get email from anil.raghuwanshi@sysnetglobal.com. Learn why this is important

AC ITS Caution: This email originated from an external sender. Be careful of phishing attacks.
Security Tip of the Month: Are your attachments secure? Before transmitting documents to another party, consider the sensitivity of the information you are attaching and whether you need to take additional steps to protect it. Safeguards such as password protecting the document(s), encrypting the email, or using a secure link to share access instead of directly attaching the records(s) are all ways you can ensure you are being a responsible information steward!

Office-365

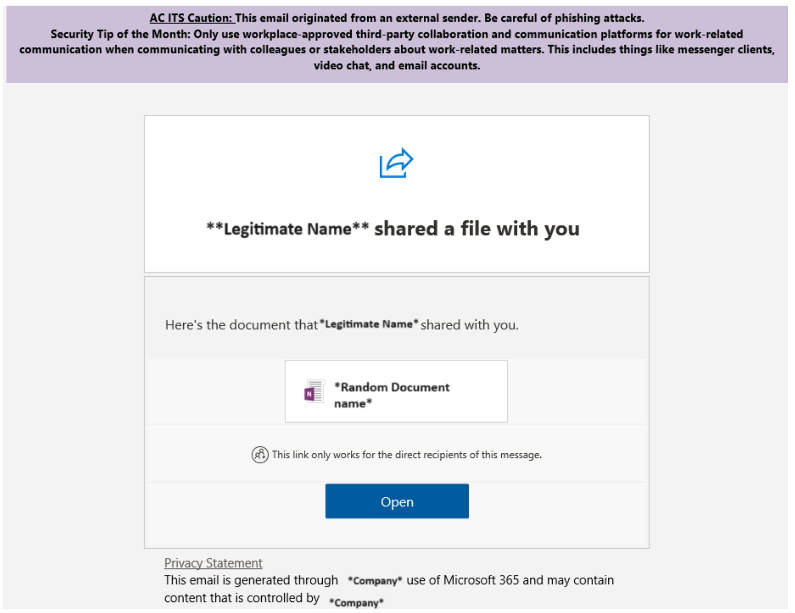
Hello dehghaa@algonquincollege.com,

Your password is due for update today.
You can change your password or keep password .

Keep Active Password

Algonquincollege Service

6



AC ITS Caution: This email originated from an external sender. Be careful of phishing attacks.
Security Tip of the Month: Only use workplace-approved third-party collaboration and communication platforms for work-related communication when communicating with colleagues or stakeholders about work-related matters. This includes things like messenger clients, video chat, and email accounts.

****Legitimate Name** shared a file with you**

Here's the document that ***Legitimate Name*** shared with you.

Random Document name

This link only works for the direct recipients of this message.

Open

Privacy Statement
This email is generated through ***Company*** use of Microsoft 365 and may contain content that is controlled by ***Company***

Common Cyber-Threats

Preventing Ransomware Attacks

What is Ransomware?

Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.

How does Ransomware work?

- **Initial Access and deployment:**
  - Gain access to your network and plant malicious encryption software.
- **Encryption:**
  - Malware is activated, locking devices and causing the data to be encrypted
- **Extortion and communication:**
  - Notification explaining the ransom demand to unlock your computer or regain access to your data.

Ransomware infection factors

1. **Phishing**
2. **Malvertising**
3. **Weak Passwords**
4. **No Multi-Factor Authentication**
5. **Unpatched Software and Systems**
6. **Insecure Remote Access**
7. **Lack of Network Segmentation**

Should I pay the ransom?

Law enforcement does not encourage, endorse nor condone the payment of ransom demands. If you do pay the ransom:

- there **is no guarantee** that you will get access to your data or computer
- your **computer will still be infected**
- you will be **paying criminal groups**
- you're **more likely to be targeted in future**

For this reason, it is important that you always practice cyber-hygiene measures that will allow you to stay safe

Common Cyber-Threats

Protecting Against Data Breaches

Ransomware: "*your data held hostage*"

It locks users out of their computer or data on drives until they pay, generally via cyber-currency, to get a key.

⚠ Risks: Critical data loss or operational shutdown unless a ransom is paid. Even if you pay, there is no guarantee of data recovery

Trojans: *"soldiers that steal"*

Seek to discover information, like financial details. They can bring in other friends like malicious code, it can also be used to take over resources to launch attacks against other devices.

⚠ Risks: Creates a hidden backdoor to access systems, allowing theft of data or further attack

Common Cyber-Threats

Protecting Against Data Breaches ....contd.

Social Engineering: *Hacking the human minds*"

Manipulating people into giving away sensitive information through deception.

⚠ Risks: Unauthorized access to sensitive data through human error, leading to data breaches or financial loss.

Password Cracking: "Breaking the Vault"

Exploiting weak password to gain unauthorized access to systems and data.

⚠Risks: Full access to systems, leading to data breaches, identity theft and unauthorized transactions.

Personal Data Hygiene

Everyday Practices for Staying Safe Online

WHAT?

Cyber or data hygiene describes the routines and habits you use to safeguard your personal information from malicious activity such as theft and cyber-attack.

WHY?

Good cyber hygiene keeps you and your personal information secure against new and emerging threats. Stay diligent!

HOW?

- **Manage your digital footprint**
- **Think before you click**
- **Use secure wi-fi networks**
- **Don’t leave your devices unattended**

Cyber Hygiene: Everyday Practices for Staying Safe Online

What is MFA?

Multi-factor Authentication (MFA) requires two or more verification steps to log in, such as:

- Something you know (Password, PIN or an answer to a secret question)
- Something you have (Phone, App, Smart Card, Token)
- Something you are (Fingerprint, Face ID)
- Somewhere you are (Location)

Benefits of MFA?

- **Stronger Security:** Even if your password is compromised, attackers can't access your account without the second factor.
- **Protection from Phishing:** Phishing attacks target passwords, but MFA ensures additional protection by requiring extra verification.
- **Stops Unauthorized Access:** Prevents hackers from accessing your accounts, even if they have your password from data breaches.

Risks of not enrolling in MFA

- **80% of data breaches** happen because of weak or stolen passwords. Without MFA, **your account can be hacked in seconds.**
- **Identity Theft:** No extra security means it's easier for attackers to impersonate you and steal personal information
- **Loss of Sensitive Data:** Not using MFA exposes your private emails, photos, and documents to potential hackers.

How to set up MFA?

Guides and MFA Resources can be found through the links below:

- Multifactor Authentication (MFA) and VPN Support for Students - ITS (algonquincollege.com)
- How to set up the Microsoft Authenticator App (site.com)

If you have any problems setting up your MFA, ITS Support is available Mon-Fri 7:30 am – 5:00 pm.

MFA will be required to all student accounts by November 2024, Sign up Today!!!

Cyber Hygiene: Everyday Practices for Staying Safe Online

What is cyber-hygiene?

Cyber hygiene refers to the habitual practices that keep your digital life safe, like how personal hygiene protects your physical health.

Importance of cyber-hygiene for Leaners

- As a student, your online life involves sharing personal data (academic, financial, and social).
- Poor cyber hygiene can lead to identity theft, data breaches, or loss of sensitive information.

Why it matters?

- Personal responsibility: You are the first line of defense in protecting your data.
- As everyone plays a role in protecting the security of the College, your actions matter.

Passwords

Do not share your password

Enable Multi-factor Authentication

Regularly change your password (<90 Days)

Endpoint

Update your software regularly

Be cautious with unofficial apps and permissions.

Install Security Software

Data

Back Up your Data

Use secure networks to access sensitive information

Verify before you trust

Cybersecurity Resources

Free Cybersecurity Tools

Passwords

Password Managers

KeePass

bitwarden

Endpoint

Antivirus

Avast One

AVG Anti-Virus

Data

VPNs

Proton VPN

windscribe

Free Cybersecurity Resources

Canadian Resources

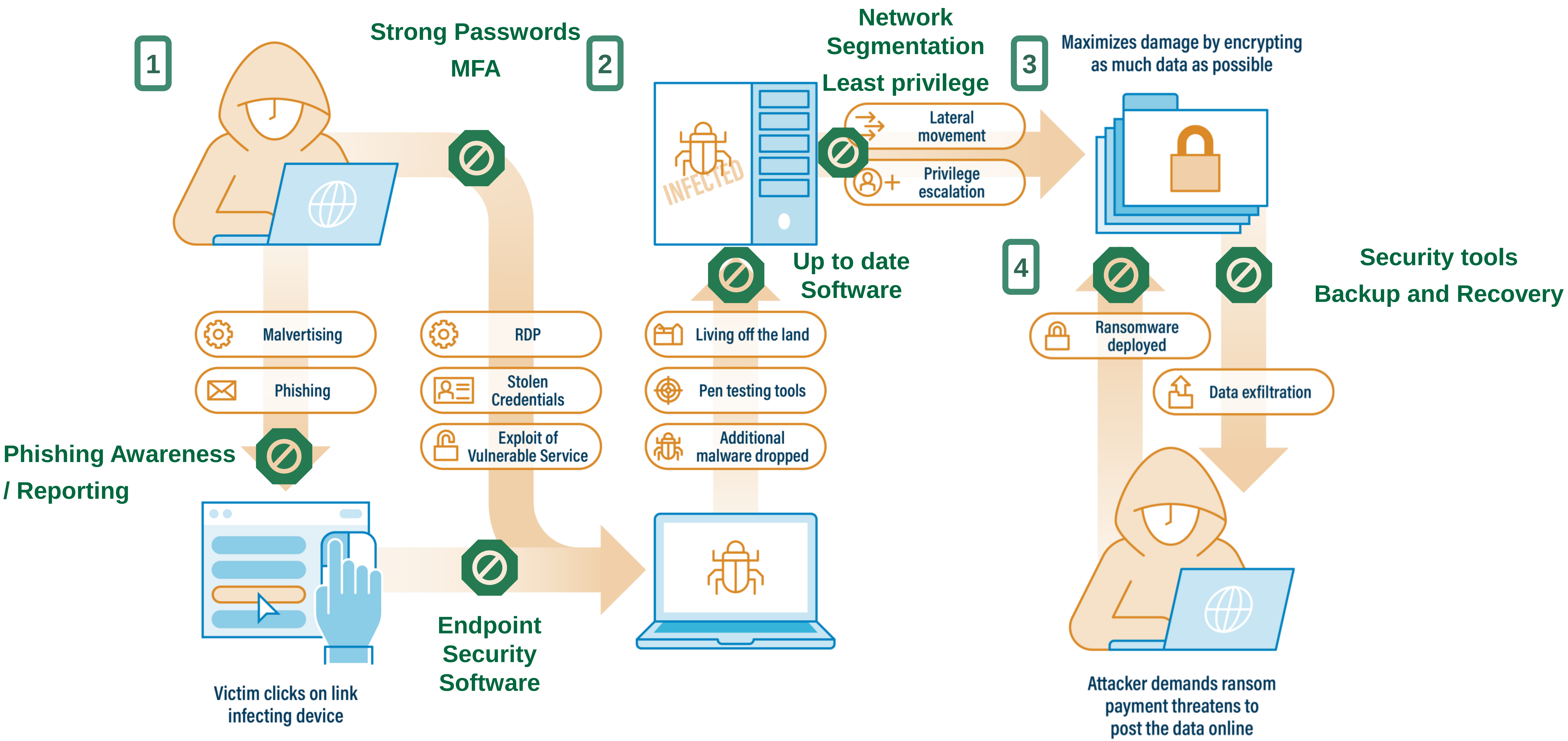
- **Get Cyber Safe:** Guides on protecting your devices and recognizing phishing.
- **Canadian Anti-Fraud Centre:** Info on phishing and identity theft protection.
- **Ontario Cybersecurity Centre of Excellence** for basics to recognize and counter threats and tips for securing information.

International Resources

- **StaySafeOnline.org:** Tips on securing your devices and data.
- **HaveIBeenPwned.com:** Check if your email/phone was in a data breach.
- **Cyber Aware:** Advice on securing accounts and staying protected from online threats

Closing Remarks

Algonquin College
Cybersecurity Awareness Month
2024



1

Malvertising

Phishing

Phishing Awareness / Reporting

Victim clicks on link infecting device

Strong Passwords

MFA

2

RDP

Stolen Credentials

Exploit of Vulnerable Service

Endpoint Security Software

INFECTED

Living off the land

Pen testing tools

Additional malware dropped

Up to date Software

Network Segmentation

Least privilege

Lateral movement

Privilege escalation

3

Maximizes damage by encrypting as much data as possible

4

Ransomware deployed

Data exfiltration

Security tools

Backup and Recovery

Attacker demands ransom payment threatens to post the data online

Closing Remarks

Key Takeaways

- **Stay Informed:** The cyber-threat landscape is ***constantly evolving***. Stay updated on the latest threats and trends.
- **Be Proactive:** Implement the best practices and defenses we've discussed to protect yourself and your data.
- **Practice Cyber Hygiene:** Incorporate everyday habits that enhance your online safety.
- **Use available Resources:** Take advantage of the shared cyber security resources available to you.

What's next?

- **Weekly awareness Newsletters:** Providing valuable tips, updates, and insights to help you stay secure online.
- **On-Campus Booths**

✓ Perth

- **Date**: Thursday, Oct. 3, 2024
- **Time**: 12 p.m. to 1:30 p.m.
- **Location**: Student Commons – Room 128.

⏭ Pembroke

- **Date:** Thursday, Oct. 10, 2024
- **Time:** 12 p.m. to 1:30 p.m.
- **Location:** Student Commons – Room 105.

⏭ Ottawa

- **Date**: Thursday, Oct. 17, 2024
- **Time**: 12 p.m. to 1:30 p.m.
- **Location**: Marketplace Food Court outside of Salon A

- Each event will feature ***freebies***, ***interactive Q&A sessions*** and ***essential best practices*** to help you ***become a digital guardian***.

Questions or Comments?

Visit our website:

https://www.algonquincollege.com/infosec/csam-2024/

Information Security & Privacy is everybody's business