CYBERSECURITY AWARENESS FOR THE MONARCH INTERNSHIP & CO-OP OFFICE

Prepared By: Samantha Riggs

WHY IS CYBERSECURITY AWARENESS IMPORTANT?

KINDS OF DATA STORED IN A UNIVERSITY'S SYSTEMS

- Personally Identifying Information (PII) for students, faculty and staff
  - Name, address, date of birth, social security number
- Academics
  - Transcripts,
  - Enrollment status and schedules
  - Honors and awards
  - Athletics participation
- Student financial information
  - Information through FAFSA such as income and documents
  - Payment and disbursement records
- Faculty HR information
  - Background checks
  - Direct deposit
  - Health insurance information

SCALE OF SYSTEMS ON CAMPUS

- Wi-Fi accessible across campus
- Diverse range of people accessing university systems and networks
  - Students, faculty, staff, and visitors as well
- Large and complex attack surface
  - Many user-owned and IoT devices, creating multiple entry points to the network
- Complex partner and vendor networks

INCIDENTS OVER THE PAST FIVE YEARS

- University of Michigan (2022)
  - 230,000 records of students, alumni, and employees were stolen because of an unauthorized party gaining access university systems

INCIDENTS OVER THE PAST FIVE YEARS

- Mount Saint Mary College (2023)
  - In December, Information was obtained and held for ransom
  - Per FBI guidance, the ransom was not paid
  - In February 2023, the information was published illegally online

Mount Saint Mary College

INCIDENTS OVER THE PAST FIVE YEARS

- University of Pennsylvania (2025)
  - Identity impersonation and social engineering
  - Compromised emails of university representatives
  - Estimated over a million records, including PII of donors, alumni, and students

University of Pennsylvania

WHAT COULD IT COST?

- Data breaches can cost a university close to $4 million[1] on average based on data from 2025
- Reputational damage
- Loss of trust
  - Students, faculty, and staff trust the institution to protect their information

1. AAG, "The Latest 2025 Phishing Statistics" , October 21, 2025

ARE THERE LAWS OR REGULATIONS TO HELP GUIDE PUBLIC INSTITUTIONS?

- Yes! There are privacy laws and regulations which must be adhered to anywhere where sensitive data is stored.
  - Family Educational Rights and Privacy Act (FERPA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Gramm-Leach-Bliley Act of 1999
    - Financial Services Modernization Act
- There are also frameworks and standards that provide guidance for how systems should be secured
  - National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - Higher Education Community Vendor Assessment Toolkit (HECVAT)

WHY IS CYBERSECURITY AWARENESS SO IMPORTANT?

- There is a factor that standards and policies can not address on a technical level
  - Estimated to be a significant component in 95%[2] of cybersecurity breaches
- That factor is human behavior and error!
- If we don't know what the risks are or what to look out for how are we supposed to know that we might be making a mistake?

2. Sentinel One, "Key Cyber Security Statistics for 2026", March 12, 2026

PHISHING

WHAT IS PHISHING?

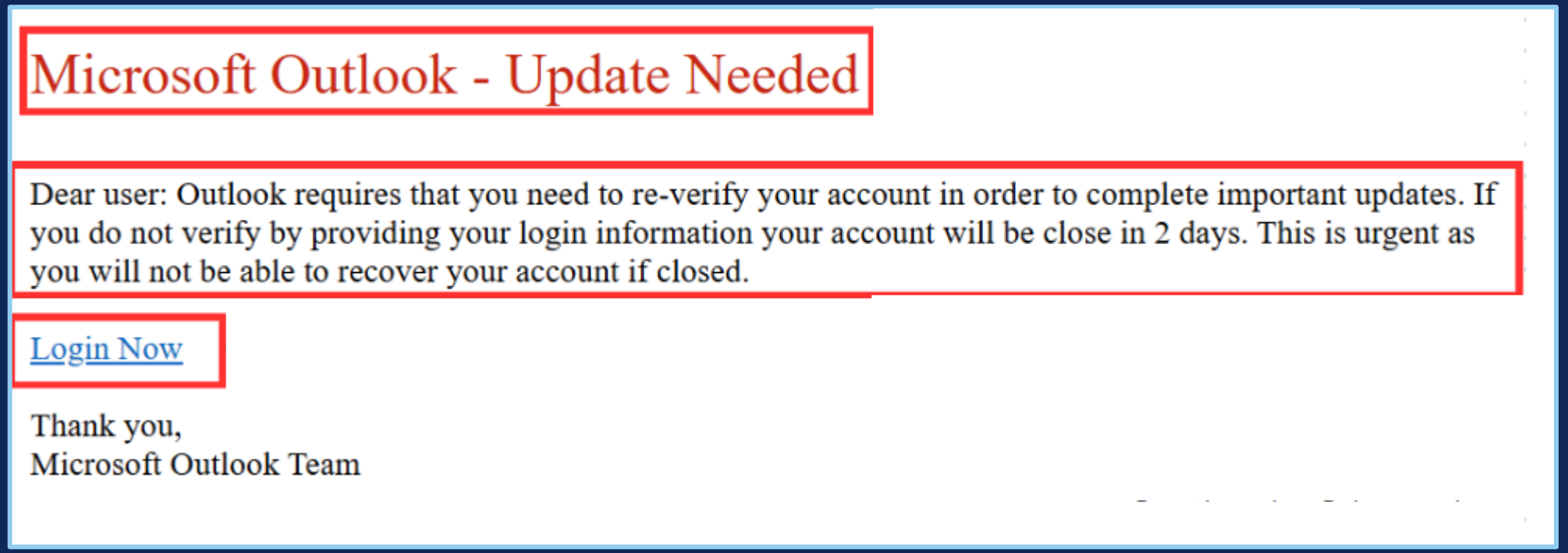
- A type of cyberattack that occurs when cybercriminals send out calls, texts, emails, or other form of electronic message pretending to be from a reputable source
- Estimated 3.4 billion[3] spam emails are sent every day

3. AAG, "The Latest 2025 Phishing Statistics" , October 21, 2025

HOW CAN I RECOGNIZE A POTENTIAL PHISHING ATTEMPT?

- Spelling and grammatical errors
- Prompts for the user to click on external links or download unknown programs
- Claims to be from within an organization, but the message originates from outside of it
- Requests sensitive information
  - Login information
  - Financial details
  - Personal information
  - Work-related sensitive information
- Includes an urgent matter that suggests that it needs to be acted on quickly

PHISHING EMAIL EXAMPLE



Microsoft Outlook - Update Needed

Dear user: Outlook requires that you need to re-verify your account in order to complete important updates. If you do not verify by providing your login information your account will be close in 2 days. This is urgent as you will not be able to recover your account if closed.

Login Now

Thank you,
Microsoft Outlook Team

HOW CAN I PREVENT PHISHING ATTEMPTS FROM BEING SUCCESSFUL?

- If any kind of message that you receive seems suspicious or has some of the warning signs described earlier:
  - Do not respond or interact with the message
  - Reach out to IT at ithelpdesk@odu.edu

- By staying vigilant and knowing what to look for, you have already prevented most phishing attempts from being successful

MALWARE

MALWARE

- Short for “malicious software”
- An umbrella term for any kind of program that is designed to disrupt, damage, or gain unauthorized access to a system
- Has the ability to steal data, encrypt files for ransom, or steal resources present on the system for the attacker’s gain

HOW DOES MALWARE INFILTRATE A SYSTEM?

- Some forms of malware can infect a system purely on a technical level alone, never needing human interaction
- However, the majority of malware requires a user's interaction in order to successfully complete its infiltration.

HOW DOES MALWARE INFILTRATE A SYSTEM

- Phishing emails
- Malicious advertisements
- Compromised or malicious website
- Malicious software bundling
- Infected physical media such as USBs

Malware Prevention

- Keep up to date with software updates
- Ensure you are utilizing some form of anti-virus software and that it is up to date
  - Windows has a pre-installed antivirus software, Windows Defender
- Avoid clicking on suspicious links or download prompts
- Practice safe browsing habits
  - Avoid suspicious sites
  - Do not click on advertisements present on sites
  - Only download software from official, trusted sources

WHAT SHOULD I DO IF I SUSPECT MALWARE?

If you:

- Notice that your device becomes unusually slow when in use
- Notice that files or programs have been changed or are missing
- Begin to see unexpected or an excessive amount of pop-up advertisements
- Know that you have interacted with suspicious links or downloaded unknown programs

WHAT SHOULD I DO IF I SUSPECT MALWARE?

- Reach out to IT at ithelpdesk@odu.edu with your concerns
- These kinds of events happening on your device do not always indicate that there is a malware infection
- It is always better to ensure that your system is secure

PASSWORD SECURITY

2021 COLONIAL PIPELINE CYBER ATTACK

- In May 2021, the fuel company had to halt its services for a span of five days due to a ransomware attack
- When the attack was investigated, it was determined that the group responsible for the attack had gained access via a compromised password for an account connected to the company's system

HOW DID A PASSWORD COME INTO PLAY?

- The employee's password in question was the same password used for a different account that had less security, and did not have multi-factor authentication enabled
- Password reuse and the consequences of not utilizing multi-factor authentication played a major role in this million-dollar ransomware event that impacted the nation

BAD HABITS

- Using the same password across different sites
- Making your password too simple
  - Short in length
  - No numbers or special characters
  - No variation of upper and lowercase letters
  - Uses simple sequences such as “password” or “123456”
- Using personal information as part of your password

PASSWORD SECURITY

- Make your passwords at least 16 characters long
  - Passwords that are of this length and are complex can be almost impossible for an attacker to determine through a brute force method
- Try to make every password unique to each account
- Do not include personal information
  - This includes names, birthdays, hometowns, or any information that be easily be found out about you
- Never share your passwords online for any reason
- Try not to write down your password and leave it where it can be seen by others

MULTI-FACTOR AUTHENTICATION

WHAT IS MULTI-FACTOR AUTHENTICATION

- Serves as a second line of defense after your password
- Requires a separate method of authentication to prove your identity and access an account
- Methods can include authentication apps, fingerprints, and whether the device you're using is your regular device

MULTI-FACTOR AUTHENTICATION BEST PRACTICES

- Have MFA enabled for all accounts
- Never approve an attempted connection or password reset request sent your set up authentication method unless you are certain it was from you
- Do not give out any MFA codes that you receive for verification

NETWORK SECURITY

TYPES OF NETWORKS

- Private home networks
- Private organizational or work networks
- Mobile access points
  - "Hotspots"
- Public networks

PUBLIC NETWORK SAFETY

- Public networks can be found at places such as restaurants, hotels, or other businesses or organizations
- Unprotected public networks are significantly vulnerable to being compromised or imitated by attackers

WHY ARE PUBLIC NETWORKS VULNERABLE?

- Malicious actors can set up a public network access point of their own and name it as if it originates from a legitimate source
  - Such as naming their fake network “Hotel Wi-Fi” within a hotel
- Once a victim connects to the fake network believing it to be legitimate the attacker gains access to data being sent to and from the Internet

BEST PRACTICES

When working remotely, or in the case that you need to access secure university systems or accounts outside of your regular work network:

- Never connect to free, unsecured, public Wi-Fi networks
- Only use Wi-Fi networks that are password protected
  - With the exception of networks that have the name and password publicly available (such as a sign at a café for customers to connect to their password protected Wi-Fi

BROWSING AND WEBSITE SAFETY

- Examine if a website looks strange or appears suspicious
  - Contains unusual font color, size or type
  - Unwanted and constant pop ups
  - Offers a product that seems "to good to be true"
- Looks for signs of legitimacy
- Read URLs carefully

- Be sure to utilize your browser's security tools
  - Ensure you have the most current version of your web browser installed
  - Most browsers have filters that can identify and warn you of potential security risks

DEVICE SECURITY

SOFTWARE UPDATES AND SECURITY PATCHES

- Operating system companies release regular software updates for their systems in order to address newly found vulnerabilities
- These are very important to keeping your device safe. If you are prompted by your system to update, do so as soon as possible. Delaying the installation of security patches leaves your device open to security vulnerabilities

PROTECTING YOUR DEVICES

- Lock your computer or any other work device while away
- If working outside of the office and using a portable device, do not leave it unattended
- Use a PIN, password, fingerprint, or any other kind of authentication barrier
- Be mindful of the kinds of applications you download to your device
  - Avoid downloading anything from untrusted or suspicious sites
- If you access work accounts outside of the workplace, ensure that you only use secure wireless networks

INFORMATION SECURITY

TYPES OF INFORMATION STORED

- We've already discussed the large and diverse range of information stored with the systems of universities
  - The sensitivity makes it appealing to cybercriminals
- Due to the sensitivity of this information, there are both technical and non-technical best practices regarding this data

TECHNICAL LEVEL BEST PRACTICES

- Verify any unexpected requests for sensitive information
- Use approved and secure methods for sharing files
  - Microsoft SharePoint
- Double-check recipients before sending emails
- Store files with sensitive information in designated, approved locations
- When dealing with third parties outside of the university, only share data verified and approved parties

PHYSICAL DOCUMENT SECURITY

- Store sensitive documents in locked cabinets or other secure location
- Limit printing of documents with sensitive data present
  - Many times, records need to be printed out or stored. This printing should be limited to an as needed basis
- Do not leave work-related documents, especially ones that have sensitive data printed on them, unattended on desks
  - Known as a “clear desk policy”
  - Prevents information being seen by an unauthorized party

INCIDENT AWARENESS AND REPORTING

- Report any suspected cybersecurity incidents immediately to IT at ithelpdesk@odu.edu
  - If an incident is confirmed, they can inform you of your next steps
- Report lost or stolen devices immediately
- Do not attempt to fix any suspected security issues independently, allow IT to assist instead

QUESTIONS?

THANK YOU!

- If you have questions and need to reach out to me about anything in this presentation or the best practices manual, feel free to contact me at srigg008@odu.edu