
# Cybersecurity Best Practices Manual

4/15/2026

Written By: Samantha Riggs

## Table of Contents

## Introduction

In today's highly complex and constantly evolving cyber landscape, technology has never been so widely accessible and sophisticated. Technology and networks are integrated into almost all aspects of our daily lives, including in the workplace, our personal lives, and in aiding our day-to-day functions. However, just because modern technology is advanced does not mean that it always is secure. As the integration of technology grows and becomes more sophisticated, cyber threats and attacks evolve in turn. The creation and subsequent strengthening of cybersecurity policies in all sectors is absolutely necessary to address the constantly changing cybersecurity landscape.

Colleges and universities are notoriously more vulnerable to cyberattacks due to various factors including their routine handling of sensitive data and their generally complex network systems. This guide is meant to provide the information and tools needed to be aware of cybersecurity threats and how to properly address them. The security of the systems present in the office is both a group and individual effort. Both parties must be vigilant and do their due diligence in order for any cybersecurity policy to be effective. Acknowledging the risks and following the best practices defined within this guide will help strengthen the Monarch Internship & Co-Op Office's cybersecurity posture and build upon Old Dominion University's overall cybersecurity landscape.

## Cyberattacks

**Cyberattack:** a deliberate and malicious attempt by an unauthorized person or group with the goal of accessing, disrupting, or damaging computer networks and systems.

There are various types of cyberattacks, each of them with their own tactics and methods of delivery. The types defined within this guide are especially important to be aware of, as they are common threats to the networks and systems of colleges and universities. These attacks are discussed in more detail later in the guide.

### Phishing and Social Engineering

Cyberattacks that use social engineering techniques use deception, coercion, or similar techniques to persuade their target to act in a certain way. This can include the impersonation of a colleague, an authority figure, a trusted vendor, or another trusted entity.

Phishing is a common form of a social engineering cybercrime in which the attacker impersonates reputable companies or individuals via email, texts, calls, or even social media in order to deceive victims into giving sensitive information or installing unauthorized programs.

### Malware and Viruses

A common and perhaps the most well-known version of malicious cyberthreat is malware, including viruses. Malware is short for “malicious software” and is defined as software that is designed and coded specifically to disrupt, damage, or gain unauthorized access into a network or computer system.

Viruses are a specific type of malware that attaches itself to programs or other files that seem legitimate in order to infiltrate their target. A computer virus functions by spreading and injecting its malicious code into other files, programs, or even the hard drive present within a system.

### Ransomware

Ransomware is a specific type of malware that encrypts a target system's files or locks the victim out of their system completely and proceeds to demand payment in order to restore files contents and system access. Attackers often gain access to systems via phishing emails, malicious websites, malicious programs, or exploiting system vulnerabilities directly.

Additionally, "double extortion" can occur. This is where the attacker also makes a copy of the sensitive data present within the compromised system. This data can then be used at a later date to threaten its release and demand another ransom.

### Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) attacks are when the normal traffic of a server or network is disrupted by an attacker overwhelming the network with internet traffic from multiple sources at once. The target server or network oftentimes is not built to handle the large flood of traffic, making the network temporarily unusable for any user.

## Cybercriminals

When discussing cybersecurity and cyber threats, it is also important to take note of the types of attackers who attempt to infiltrate or compromise networks and systems. These different types differ in their number of resources and sophistication of their methods, but all types of attackers have the ability to pose a legitimate threat. It is important to note that some of these types are less likely to be a direct threat to ODU, but it is still integral to cybersecurity awareness as a whole to acknowledge them.

**Cybercriminals**

- Individuals or organized groups
- Primarily motivated by financial gain

**Insider Threats**

- Can be employees, partners, or contractors
- Have authorized access, but misuse it for personal gain

**Amateur Hackers**

- Inexperienced individuals, otherwise known as “Script Kiddies”, that utilize pre-written scirpts
- Conduct cyberattacks for personal enjoyment or for reputation

**Hacktivists**

- Hackers motivated by political or social causes
- Primary goal of disrupting services or leaking information for the purpose of raising awareness

**Nation-State Actors**

- Government-backed hackers
- Conduct espionage, theft of intellectual property, or sabatoging

## Phishing

Phishing is a type of cyberattack that occurs when cybercriminals send out calls, texts, or emails pretending to be from a reputable source. Phishing messages rely on social engineering tactics that aim to influence the human user as a means of infiltration versus the system itself. Phishing is extremely common when an estimated 3.4 billion spam emails are sent every day. This notable number is due in part to how simple it is to send on a large scale.

### How Can I Recognize a Potential Phishing Attempt?

Phishing messages can be hard to spot if you do not know what to look for. Phishing attempts often appear to come from a trusted source, enforcing a sense of urgency to convince you to react quickly without taking the time to consider the message's legitimacy.

- **Spelling and grammatical errors**

There will often be spelling or grammatical mistakes within the message.

- **Prompts for the user to click on external links or download unknown programs**

The links present within a phishing attempt can lead to unsecure, fake websites in order to steal your information. These websites can often look identical to one it is trying to imitate. Additionally, these links can download files or programs to your computer, which can carry malware and infiltrate your system.

- **Claims to be from within an organization, but originates from outside of it**

Outlook will often alert you when you receive an email either from someone outside of ODU's internal email system or from someone that you do not often receive mail from in order for you to exercise extra caution. Any email or message claiming to be from someone within the university that does not have @odu.edu in the sender's address should raise a red flag.


*An example of an Outlook alert you may see if you receive an email either from someone outside of ODU's internal system or some someone you do not often receive mail from.

- **Requests sensitive information**

Some emails will request sensitive information from you. It is important to note that no reputable company or organization will **ever** ask for this kind of information through email, text, or phone.

Some examples of information a phishing message may ask for include:

**Login Information**

- Username
- Password

**Financial Details**

- Credit card number
- Bank account number
- Logins for banking websites or apps

**Personal Information**

- Date of Birth
- Social Security Number
- Home Address

**Work-Related Information**

- Usernames and passwords for work accounts
- Access codes for internal systems

- **Includes an urgent matter that needs to be acted on quickly**

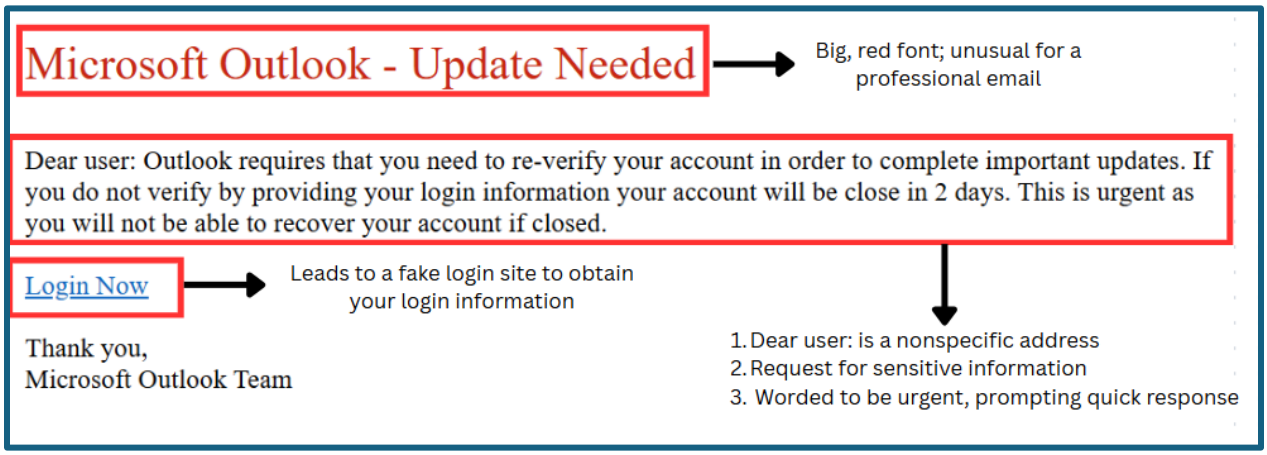
Phishing attempts will often use wording that insinuates urgency and potential consequences in order to elicit a hurried response from the victim. These kinds of messages also often come with a demand for reverification of an account (to obtain login information) or immediate payment (to obtain your financial information).

**Example**

Emails are the primary method of delivery for phishing attempts, especially within institutions like ODU, that utilize software like Outlook for their daily workflows. For this

reason, an email will be used as an example. Keep in mind that phishing texts, calls, or any other kind of message will generally share the same structure and warning signs.

Hypothetically say that you received this email in your inbox:




The example here may seem like an obvious phishing attempt due to the format and amount of warning signs present, but it is important to keep in mind that a real phishing attempt may only have one or two of these signs.

### How Can I Prevent Phishing?

If any kind of message that you receive seems suspicious or has some of the warning signs above, do not respond to the message and reach out to IT services to report it. This also applies if you receive a message and are simply unsure of its legitimacy. IT services will be able to help you identify if a message is legitimate.

It is always better to stop and take the time to confirm that a potentially suspicious message is authentic rather than responding right away. Remember, these kinds of attacks rely on human behaviors and responses in order to be successful. By being aware of what phishing attempts can look like and knowing when not to respond and when to report, you have already prevented the attempt from being successful.

## Malware

Malware is short for “malicious software” and is an umbrella term for any kind of program that is designed to disrupt, damage, or gain unauthorized access to a system. Malware has the ability to steal data, encrypt files for ransom (ransomware), or steal resources present on the system for the attacker’s gain.

## How Does Malware Infiltrate a System?

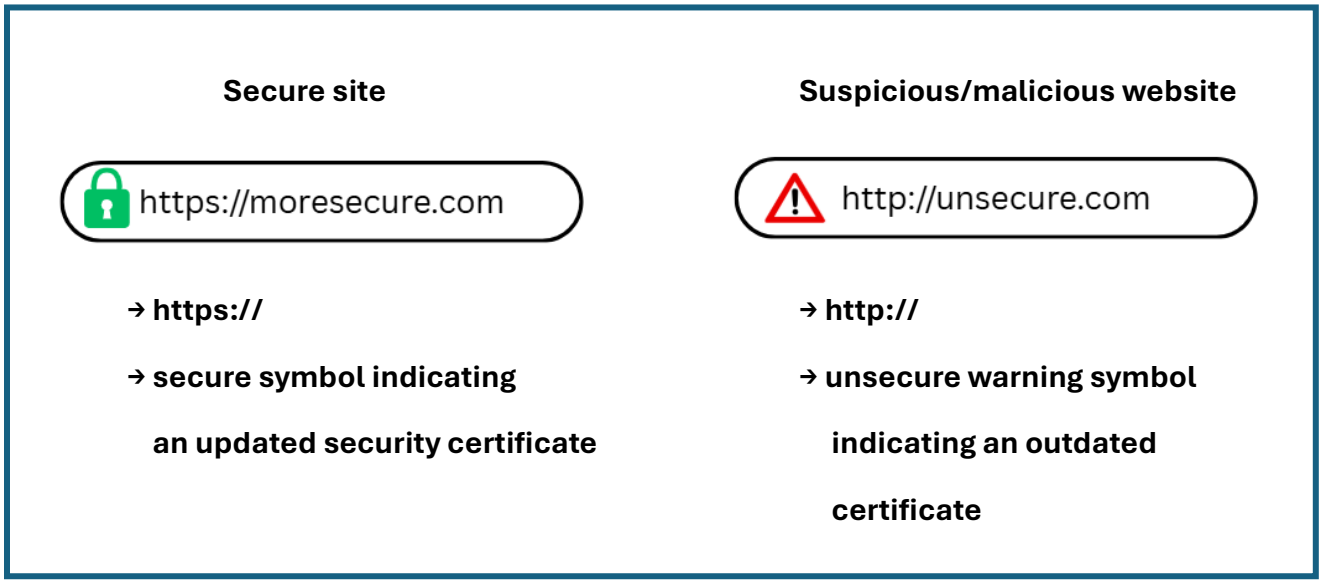
Malware can infiltrate a system in various ways. Some forms of malware have the ability to infiltrate a system on a technical level alone, never having to have human interaction. However, the majority of malware requires a user's interaction in order to successfully complete its infiltration.

- **Phishing emails**

Phishing emails, texts, or other kinds of messages attempt to trick users into clicking malicious links, entering credentials, or downloading infected files. These messages often pretend to be from trusted sources like work colleagues, banks, or police departments.

- **Compromised or malicious websites**

Websites that are compromised allow malware to be installed automatically on a user's system through unpatched browser or plugin vulnerabilities. This method of infection often does not require the user to click or interact with anything.



- **Malicious advertisements**

Malicious advertisements can be placed on legitimate websites that redirect users to malicious sites or download the malware upon being clicked.

- **Malicious software bundling**

Malware can be hidden within legitimate software installers, pirated content, or free downloads online from untrusted sites.

- **Infected physical media**

Some forms of malware can infect physical media such as USB flash drives and can then be spread from device to device.

## How Can I Prevent Malware Infection?

The easiest way to prevent malware from infiltrating your device is to not provide an opening for infection. Remember, most malware requires human interaction to infect a device or network. Awareness of the methods of infiltration and the subsequent prevention methods is key.

### 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 operating**
- **Begin to see unexpected or an excessive amount of pop-up advertisements**
- **Notice that files or programs have been changed or are missing, or,**
- **Know that you may have interacted with unknown links or downloaded unknown programs,**

reach out to IT services with your concerns. These kinds of events happening on your device does not always mean that there is a malware infection, but as with the common theme in this guide, it is better to ensure that it is not the case.

## Password Security

Passwords are integral in authenticating our identities for all of our accounts. They ensure that the contents of our accounts stay secure and that only those who are authorized have access to that content. However, password security is often overlooked and has been a component of cyber attacks in the past.

A significant example is the Colonial Pipeline ransomware attack. In May 2021, the fuel company had to halt its services for five days due to a ransomware cyberattack. This severely impacted operations and fuel distribution across a wide area within the United States. When the cause of this attack was investigated, it was determined that the group responsible had gained access by exploiting a compromised password for an employee's account, which did not have multi-factor authentication enabled, connected to the company's systems. This exploitation was aided by the fact that the employee whose password had been compromised used the same password for their work account that they had for a separate account that became compromised first. This allowed the attackers to access Colonial Pipeline's systems without needing to bypass the security on a technical level. This matter of password reuse played a major role in this million-dollar ransomware event that impacted the nation.

## Bad Habits

Due to the idea of simplicity and convenience, many people fall into these bad habits when creating passwords for their accounts:

- **Using the same password across different sites**

If the password for one of your accounts becomes compromised, then the rest of your accounts that share the same password are now unsecure.

- **Making your password non-complex**
    - **Short in length, no numbers, no special characters, no uppercase/lowercase mixture**

Attackers have the ability to perform brute-force attacks through programs that try different combinations in order to determine passwords. The more complex a password is, the longer it will take for an attacker to crack. The idea behind password complexity is to make the length of time and effort involved with cracking the password outweigh the end result for the attacker. If a password is complex enough, a brute-force attack will be impossible to carry out given the amount of time that would be required to determine the password, only leaving more complex methods for an attacker to use.

- **Using personal information as part of your password**

Passwords that use personal information, especially information that can be easily found out such as names and birthdays, are more vulnerable to being guessed or discovered.

## Best Practices

Many companies and organizations implement password requirements when a user is creating their password in order to help facilitate the creation of hard to crack passwords. Regardless of the presence of mandatory requirements, it is still highly recommended to follow these best practices.

Secure passwords should:

- **Be at least 16 characters long**

- **Be unique to every account**
- **<u>Not</u> include personal information including birthdays, names, or hometowns**
- **<u>Not</u> include simple sequences such as "123456" or "password"**

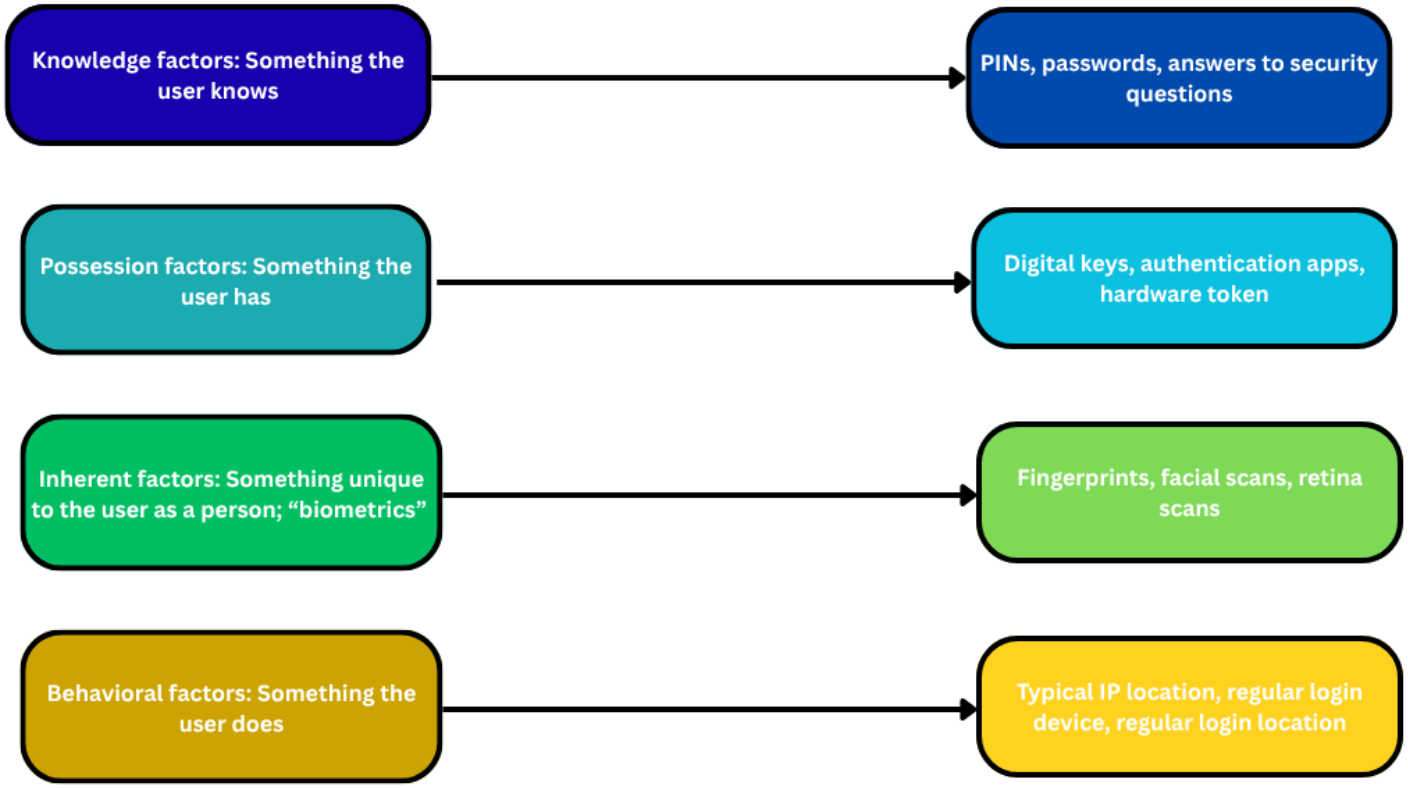
Additionally:

- **Never share your passwords**
- **Try not to write down your password and leave it out in the open where others can read it**

## Multi-Factor Authentication

As cyberattacks have become more sophisticated, passwords (even highly complex ones) are able to be compromised through methods such as obtaining them through data leaks, keystrokes, and brute force guesses.

Multi-factor authentication (MFA) serves as a second line of defense, requiring a separate method of authentication other than a password in order to access an account. MFA is also known as Two-Factor Authentication or Two-Step Verification. Authentication factors are required in MFA to prove a user's identity. The user should be able to provide at least two forms of authentication factors from two different categories.




## Best Practices

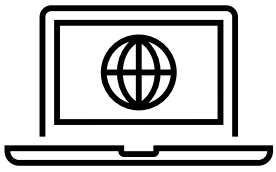
MFA has proved to be a very efficient method in securing accounts and their data, but it is not foolproof. Cybercriminals can sometimes bypass MFA, but it is much more difficult and more effort to get into an account with MFA versus an account that only uses a password. Here are some best practices to follow:

- **Have MFA enabled for all of your accounts**
- **Never approve an attempted connection or password reset request sent to your MFA method unless you know that it was from you**
- **Do not give out any MFA codes that you receive for verification**

## Network Security

Computers and mobile devices have the ability to connect to several different types of networks. These connections are used to access the Internet or to access an organization's servers and have various levels of security. These connection types include:

- **Private home networks**
- **Private organizational/work networks**
- **Mobile access points ("hotspots")**
- **Public Wi-Fi**



## Public Network Safety

Public Wi-Fi networks can be found at places such as restaurants, hotels, or other kinds of businesses or organizations. These kinds of networks can pose a security risk as they can be compromised or imitated by attackers. Malicious actors can set up a public network and then name it as if it was from a legitimate source (such as naming their fake network "Hotel Wi-Fi" in a hotel). Then, once a victim connects to the fake network thinking that it is legitimate, the attacker can gain access to any unencrypted data being sent to and received from the Internet, and even attempt to intercept sensitive, encrypted data.

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

- **Avoid connecting to free, unsecured, public Wi-Fi networks.**
- **Only use Wi-Fi networks that are password protected.**

*However*, be mindful that if the network name and password are in a place where everyone can see (such as a sign at a café that informs customers of the Wi-Fi name and password), a cybercriminal can still set up a malicious access point that mirrors the legitimate one with the same password.

## Browsing and Website Safety

- **Examine if a website looks strange or seems suspicious**

Utilize common sense. If a website looks odd, such as containing unusual font color, size, and type, unwanted or constant pop ups, or is offering a product that seems “too good to be true, exercise caution.

- **Look for signs of legitimacy**

If the website is meant to be for business, try to find contact information or some real-world presence.

- **Read URLs carefully**

Malicious websites can mirror legitimate websites while having very similar domain names. For example, if you were trying to access Google, but typed “goggle.com” instead in the URL bar, you may encounter a website that either looks identical to Google in order to log your searches into the fake search engine or directly access a malicious website with pop up malware.

- **Be sure to utilize your browser’s security tools**

Ensure that you have the most current version of your web browser installed. Most browsers have filters that can identify and warn you of potential security threats while browsing the web.

# Device Security

## Software Updates and Patches

Operating systems and companies release regular software updates for their systems. New vulnerabilities are constantly being found, and in response, operating system companies have to create a patch and defense against them before cybercriminals can exploit those vulnerabilities further. While regular updates can be inconvenient, especially if it seems like they are always needing to happen or seem to consistently interrupt your work, they are very important to keeping your device up to date and best protected on a technical level.

If you are prompted by your system to update your device, **do so as soon as possible.** Delaying update installation to leave your device open to security vulnerabilities.

## Protecting Your Devices

- **Lock your computer or any other work device while away**

This also applies in cases where you may be using a personal device to access work accounts outside of the workplace. When devices are left unattended, they become vulnerable to theft or sensitive information being obtained by unauthorized parties.

- **Use a PIN, password, fingerprint, or any other kind of authentication barrier to protect your computer**

- **Keep up to date with software updates and security patches**

- **Be mindful of the kinds of applications you download to your device**

Before downloading any new applications, take the time to exercise caution and 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**

Secure wireless networks are protected by a password that is not publicly available. Any unprotected public network is very vulnerable to being compromised.

## Information Security

### Types of Information Stored Within Systems

Higher education institutions, including ODU, are entrusted to a large and diverse amount of sensitive information. The sensitive nature of this data makes it appealing and valuable to cybercriminals. This information includes:

**Personally Identifying Information**

- **Date of Birth**
- **Name**
- **Address**
- **Social Security Number**

**Academic Information**

- **Transcripts**
- **Class Schedules**
- **Enrollment Status**
- **Honors and Awards**
- **Athletics and Club Participation**

**Financial Information**

- **Payment Methods**
- **Obtained FAFSA Information**
- **Disbursement and Refund Records**

**Human Resources Information**

- **Direct Deposit**
- **Background Checks**
- **Health Insurance Information**

### Technical Best Practices

The following are best practices that should be followed when dealing with sensitive information stored on computers or servers:

- **Verify unexpected requests for sensitive information**
- **Use approved and secure methods for sharing files**
- **Double-check recipients before sending emails**

Ensure the recipient is who you are intending on emailing, especially if it deals with sensitive information

- **Store files with sensitive information in designated, approved storage locations**
- **When dealing with third parties outside of the university, only share data with approved vendors**

## Physical Document Security

This information can, and often is, printed out and kept within the contents of physical documents as well. In this case, the following best practices should be adhered to:

- **Store sensitive documents in locked cabinets or other secure locations**
- **Limit printing of sensitive materials**

Many times, records need to be printed out and kept for various purposes. This point is meant to highlight that the printing of documents containing sensitive information should be limited to an as needed basis.

- **Do not leave work-related documents, especially ones that have sensitive information printed on them, unattended on desks**

This is known as a clean desk policy, and prevents information being seen by any unauthorized party.

## Incident Awareness and Reporting

In the case of a suspected incident regarding a data breach regarding sensitive information:

- **Report any suspected data breaches immediately**
- **Report lost or stolen devices immediately**

- **Do not attempt to fix security issues independently, reach out to IT for assistance instead**

Remember that everyone must play their part in protecting the sensitive data entrusted to the Monarch Internship & Co-Op Office by students, colleagues, and employers. Doing so includes being vigilant about who is allowed to view and receive certain sensitive information and not freely giving out information to unknown parties. When in doubt about the identity of someone requesting information or if the person is authorized to handle said information, reach out to IT at ithelpdesk@odu.edu or upper management.

## Conclusion

Cybersecurity is not a simple one-time effort, but an ongoing commitment. The practices outlined in this manual are designed to reduce risk and promote a culture of strong cybersecurity awareness across the Monarch Internship & Co-Op Office. Cybersecurity practices are most effective when they are proactive, adaptive, and shared as a collective responsibility. Taking this fact into account, it is integral that we all do our part in protecting the data stored within Old Dominion University's systems that have been entrusted to the university by students, faculty, staff, alumni, and donors.

If you have questions regarding the content of this manual, please feel free to contact me at srigg008@odu.edu.

## References


Cyberattacks

Jonker A., Krantz T., IBM, "What is a cyberattack", n.d.

IBM Cloud Team, IBM, "Types of cyberthreats", n.d.

Cybercriminals

Canadian Centre for Cyber Security, "An introduction to the cyber threat environment", n.d.

Phishing

Check Point, "Social Engineering vs Phishing" , n.d.

Microsoft Support, "Protect yourself from phishing" , n.d

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

Malware

Fortinet, "Types of Malware: How to Identify and Defend Malware", n.d.

Cisco, "How to prevent malware attacks", n.d.

Boston University, "How to Identify and Protect Yourself from an Unsafe Website" , n.d.

Password Security

Insurica, "Cyber Case Study: Colonial Pipeline Ransomware Attack" , n.d.

UC Santa Barbara Information Technology, "Password Best Practices", n.d.

Device Security

Cisco, "What Is Device Security?", n.d.

Information Security

Cybersecurity & Infrastructure Security Agency, “Cybersecurity Best Practices”, n.d.

SentinelOne, “Cyber Security Best Practices for 2026” , n.d.