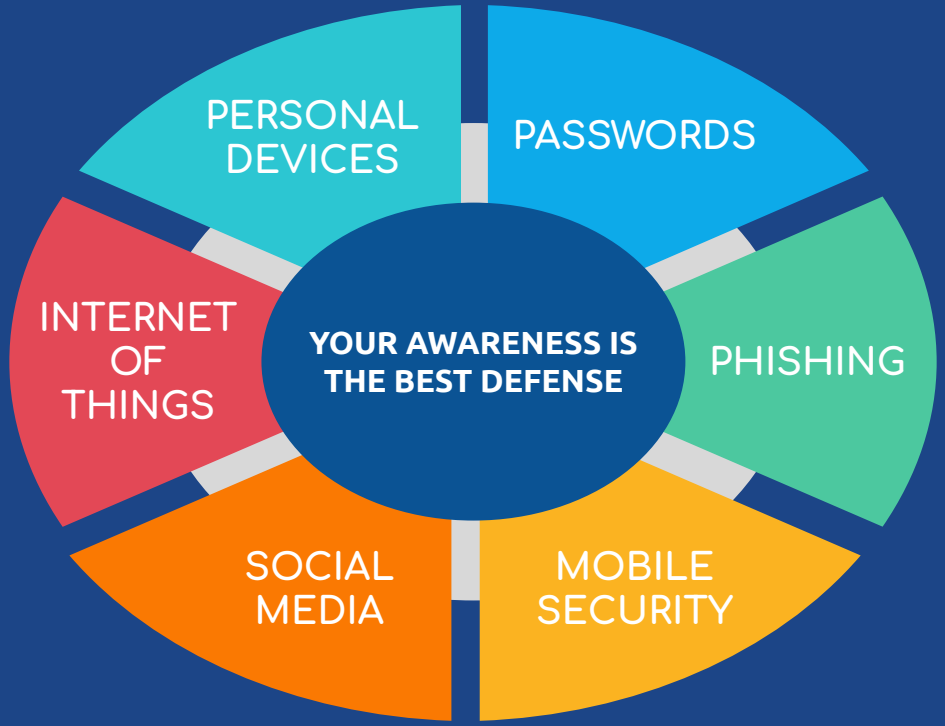
Cybersecurity Awareness Topics & Best Practices For Maintaining Robust Digital Hygiene



GUARDSIGHT
https://www.guardsight.com

For additional advice or to learn more contact us: info@guardsight.com

Malware is a generic term for malicious software installed without consent on a device designed to compromise the device's integrity. Malware is meant to give attackers access to your device and its information or serve as a pivot point to access other devices. Attackers want this access to control your online activity, steal your personal information and other sensitive data, or impersonate you to trick others into trusting requests that appear to be legitimately from you.

What To Be Aware Of:

Personal devices can be targets for malicious software (malware), used to gather information from personal devices to be used in subsequent cyber-attacks and as a pivot point to gain access to other devices and assets.

How To Protect Yourself:

- Maintain the latest operating system and application (e.g., browser) patches, and security software
- Inspect and update networking devices frequently, including routers, firewalls, and wireless products
- Reduce your attack surface by removing data stored on personal devices valuable to cyber attackers
- Implement strong multifactor authentication when using internet-based applications and services
- Utilize a cloud service to encrypt and securely store critical personal files remotely
- Learn how to review the logs produced by personal device activity
- Prune applications not being used often to reduce your device attack surface
- Avoid installing feature-rich applications that have only free services - if it's free, you are the product!
- Think about how you protect assets in the natural world and apply that same skill in the digital world
- Use common sense - if it seems suspicious or dangerous, it probably is!

For additional advice or to learn more contact us: info@guardsight.com

Passwords remain the prevalent authentication method used to access online applications and services. Cyber attackers take advantage of poor password hygiene and weak password security to compromise systems (e.g., email). Attackers will use automated tools to access assets where you use the same password and fail to use multifactor authentication. Attackers want this access for use in subsequent attacks, including trust violations and elevation of privilege.

What To Be Aware Of:

Passwords can be targets for attackers to gain what appears to be legitimate access to online applications and services. Attackers often depend on users to *reuse* the same password for multiple services multifactor authentication.

How To Protect Yourself:

- Use online applications and services that support multifactor authentication, especially for those that are used for personal information, sensitive data, and company resources
- Use a password manager to generate a unique set of characters for each online application or service
- When generating passwords for personal memory (e.g., a master password for a password manager), use phrases, mixing case, using punctuation and symbols, substituting numbers for letters, and substituting phonetic replacements for letters (ISee@!!Ph0urSeas0nZ)
- Change your passwords frequently (e.g., consider using forgot password features), including master passwords used in password managers
- Treat passwords as personal and private, and avoid sharing passwords!

For additional advice or to learn more contact us: info@guardsight.com

The majority of data breaches begin with a phishing attack. Phishing attacks use email, telephone, or text messages to lure individuals into providing sensitive data for use in subsequent nefarious activities such as providing sensitive information or installing malware without full consent. Cybersecurity experts project that phishing will continue to be a primary vector used by attackers for the foreseeable future.

What To Be Aware Of:

Cybercriminals recognize phishing as a remarkably effective method to begin a successful cyber attack. Phishing attacks depend on an intermediary: you! Your awareness is the best defense!

How To Protect Yourself:

- Avoid reading email, text, or voice messages from unknown sources that convey a sense of urgency, or crisis laden deadlines could be a phish
- Mark suspected phishing as spam or delete the message without engaging the sender
- Disable automatic display of images or files within email client; implicit acceptance of these resources signals to the sender that the recipient (you) exists and may participate if communication persists
- Beware of the possibility that suspicious requests from trusted senders may be the result of those senders being compromised
- Participate in phishing simulations to get better at recognizing what attacker activity looks like
- Use common sense - if it's too good to be true or unusual - it probably is!

For additional advice or to learn more contact us: info@guardsight.com

Cyber attackers know that targeting you and your mobile devices (e.g., phones, tablets, smart watches) may be the path of least resistance to accomplishing their objectives. They'll often try and trick you by offering apps that you believe are useful or exciting to gain access to your device. Even trusted sources are using your personal information in ways you may not understand. Only download apps you need and if you must use the app, obtain it from trusted sources.

What To Be Aware Of:

More than 50% of mobile users uninstall, or decline to install, mobile apps due to concerns about abuse of their personal information or their digital hygiene. Only use apps you need and if you must use an app, obtain it from a trusted source.

How To Protect Yourself:

- Only download mobile apps that you need and obtain those from trusted sources
- Ensure that system and apps auto-updating features are enabled on all mobile devices
- Use a pattern/biometric to lock/unlock mobile devices
- Reduce your attack surface by removing data downloaded and stored on mobile devices that could be valuable to cyber attackers (e.g., company reports, personal financial statements, health information)
- Think "residue" and periodically inventory your device to remove residue
- Prune mobile apps not being used often to reduce your device attack surface
- Think "single-use" when installing an app for temporary use and uninstall it after that single-use
- Avoid installing feature-rich applications that have only free services - if it's free, you are the product!
- Use common sense - if it seems suspicious or dangerous, it probably is!

For additional advice or to learn more contact us: info@guardsight.com

Cyber hoodlums may create targeted social engineering campaigns against you designed to gain access to your sensitive work and personal data by harvesting information found on social media platforms. Social engineering uses deception to manipulate individuals into divulging confidential or personal information. Think beforehand about what you share on social media and how threat actors might accumulate that for fraudulent purposes.

What To Be Aware Of:

Nearly four billion people use social media, and they typically use more than one platform. These platforms represent an attack surface saturated with an often vulnerable component that cyber attackers routinely attempt to exploit: humans.

How To Protect Yourself:

- Own and take control of your privacy; think before you share and communicate on social media
- Reduce your attack surface by pruning/limiting the number of social media accounts you maintain and interact with; think - “do I need this social media account?” or “do I have to comment on this?”
- Think beforehand about what you share on social media and how threat actors might accumulate that for fraudulent purposes; if you think you’re providing too much information (TMI), you probably are!
- Regularly review and update the privacy settings on all of your social media accounts; social media companies may override those desired settings when they add feature enhancements
- Never post sensitive information or personally identifiable information to social media
- Implement strong multifactor authentication for accessing your social media accounts
- Beware of the benevolent social media platforms - you, and your privacy, are the product!

For additional advice or to learn more contact us: info@guardsight.com

The Internet of Things (IoT) is a term used to describe the billions of devices embedded with sensors and actuators internet-connected through global networks. Attackers want access to these devices to control environments, create botnets, steal sensitive data, endanger, spy, manipulate, injure, and extort. These devices provide convenience in our lives, but they require a vast amount of information sharing to do so. Think "*protect before you connect.*"

What To Be Aware Of:

Twenty-five billion IoT devices (automobiles, wearables, voice assistants, cameras, ...,) are internet-connected, and coupled with 150 new devices added every second makes the IoT ecosystem an attractive and large target for cyber miscreants.

How To Protect Yourself:

- Change the default administrator passwords on your home IoT devices
- Ensure that system and apps auto-updating features are enabled on all IoT devices
- Use strong passwords, and if possible multifactor authentication, for IoT user accounts
- Segment your home IoT devices from your home data networks (e.g., laptops, phones, printers)
- Purchase from reputable companies that promote privacy and security related to their IoT products
- Learn how to review the log data produced by your IoT device activity
- Think about the data you're sending to IoT vendors and make sure you trust them to protect it
- IoT devices typically include a mobile application for managing the device; beware that apps on your mobile device that have nothing to do with your IoT devices may be gathering IoT information in the background due to your acceptance of the default permissions of those apps

For additional advice or to learn more contact us: info@guardsight.com