Virus: A virus is a malicious program that can replicate itself and spread to other computers by attaching itself to legitimate files. It can cause damage to data or hardware, and may even steal personal information.

PREVENTIONS:

\*Keep your computer up to date

* All operating systems on computers get frequent updates that enhance features but also include security patches that will fill security holes before cyber criminals do.

\*Don’t use Internet Explorer

\*Backup your computer

* With your data backed up, the process of virus removal is quicker and more affordable. We recommend backing up all of your data, with sensitive information having priority.

\*Anti-virus Basics

* Anti-virus software is the basis of computer virus protection — hence the name. While it’s important to have a quality anti-virus installed on your computer, there are some best practices to have in mind.

\*Avoid Suspicious Website

* Be sure to notice the URL of the web site, check on official sources if the website is real and actually is what it presents like. While obvious, the lock icon next to a URL is one of the first signs that you might be on a potentially malicious website.

Always Scan Email Attachments

* The most reliable way to make sure you are safe is to open an email attachment or click on a link is to scan it with anti-virus software. Your mail provider or email service you are using should also have some sort of email protection against viruses. In Gmail, for example, attachments are automatically scanned for viruses. If a virus is present, the email will be rejected and you will be notified.

Use Malware Scanner

* In order to make sure viruses don’t get the opportunity to spread further through your network and to minimize the damage, a weekly malware scan should be scheduled.

Trojan: A Trojan horse is a type of malware that appears to be a harmless program but is designed to cause harm to a computer system or steal information. It often comes in the form of an email attachment or a software download.

PREVENTIONS:

\*Be careful when downloading

* You should never fully trust the download or installation of software from the websites.

\*Be alert of threats of phishing

* Never open an appendix, click a link, or execute a program that you don’t know about in an email.

\*As soon as updates are available, upgrade your operating system software

* You should also review other software updates that you use on your computer in addition to operating system upgrades. Security patches are regularly used for updates to protect you against dangers.

\*Don’t visit websites that are unsafe

- Look for websites with safety certificates — the URL should start with https:// instead of http://, the “s” means “secure” and the padlock emblem should also be in the address bar.

\*Avoid clicking on pop-ups or banners

- Do not click on the unknown, unreliable pop-ups that warn you that your device is infected or that it offers a miracle solution. This is a common tactic of a trojan horse.

Worm: A worm is a self-replicating malware that can spread rapidly across a network. It can cause damage to data and hardware, and may even overload a network's resources.

PREVENTIONS:

* Keep your computer up to date by manually updating Windows or letting it install automatic updates. This can have a substantial impact on limiting your security vulnerabilities.
* Use some kind of antivirus or anti-malware software. You can use the virus and thread protection built into Windows or employ more comprehensive third-party antivirus apps.
* Be careful when you click links and open attachments. The same advice always applies when it comes to malware: Never click or open anything you do not trust, whether it's in an email or on a website.

Spyware: Spyware is a type of malware that secretly collects personal information from a victim's computer. It can record keystrokes, take screenshots, and even steal login credentials.

PREVENTIONS:

\*Deter Downloads

* Walk this line carefully: Don't let friends and family - especially the tech neophytes like your grandmother - download anything. Then download and install the Google Toolbar for them.

\*Teach Back-up and Restore Basics

-Teach users how to create restore points in XP and to set one before every download from a Web site that's not a brand-name portal. Disk space shouldn't be a problem on newer PCs, but even if they fill up their hard disks, eliminating some restore points is much easier than cleaning a spyware infection.

\*Create a Spyware Removal CD

* Make your own spyware tool kit by burning a half-dozen spyware utilities to CD.

\*Run at least two Spyware Cleaners

* Run several utilities, run them regularly, vary them and make sure they're all up to date. Paid cleaners provide more constant signature file updates, but even freeware adds new capabilities regularly. Run, update, run, update, repeat. I clean a system, reboot into Safe Mode and clean it with a second tool, then reboot again.

\*Close desktop communication holes

* Look for products that do stateful packet inspection of incoming and outgoing packets. A combination of personal firewall and router controls isn't overkill, especially for users who can't resist the lure of spyware-laden sites.

\*Deal with Digital Rights Management (DRM)

* One answer is to avoid DRM applications such as music players, especially those from Microsoft. If you prefer your music, get a resident commercial spyware utility that updates its spyware database regularly because it will coordinate protection with the music services.

Leverage AOL Membership

* Spyware protection from AOL, free for download for AOL members, is another useful addition from AOL as it continues to regain relevance. AOL offers some valuable protections for families, such as parental controls, but its browser is based on Internet Explorer and therefore suspect.

Keylogger: A keylogger is a type of malware that records a victim's keystrokes, often to steal login credentials or other sensitive information.

PREVENTIONS:

\*Use a Firewall

* The Windows Firewall is an excellent option for most users, but several excellent third-party firewall options come with extensive functionality. A firewall alone might not stop a keylogger or its associated malware, but it is better to have one than not.

\*Install a Password Manager

* The point of a password manager wasn't to stop keylogging. However, if you do encounter a keylogger and you have a password manager installed, there's a chance you only lose the strong single-use password for one account, rather than every password for every account you own.

\*Update your System

* Being proactive about system security is always a good idea. One of the most important parts of a proactive defense is keeping your system up to date. That includes your operating system as well as the applications and programs you run on it.

\*Consider Additional Security Tools

* Ghostpress: a free anti-keylogger with an extremely small performance footprint. Features Process Protection to stop any other program terminating Ghostpress.
* KL-Detector: a basic keylogger detection tool. Once you detect a keylogger, it's up to you to remove it, but the tool will alert you to the keyloggers presence.

\*Change Your Password

* Frequently changing your passwords will help minimize the potential damage of a keylogging attack. Your password may be stolen, but it would be uncommon for it to be stolen and used immediately unless that keylogger was targeted directly at you (in which case you may have bigger problems than keylogging!). If you change your password every two weeks, your stolen information will no longer be useful.

**WORST TYPES OF MALWARES**

Ransomware: Ransomware can encrypt valuable files and data, making them inaccessible to the victim. It can be challenging to recover from a ransomware attack without paying the ransom or restoring from a backup.

PREVENTIONS:

\*Never Click on Unverified Links

* If a link is in a spam email or on a strange website, you should avoid it. Often, hackers spread ransomware through a malicious link that initiates a malware download. If a link has not been verified, it is best to leave it alone.

\*Scan Email for Malware

* How to stop ransomware virus or other malware starts with scanning email communications. Email scanning tools can often detect malicious software. After the scanner has detected malware, the email can be discarded, never even reaching your inbox.

\*Use Firewalls and Endpoint Protection

* Firewalls can be a good solution as you figure out how to stop ransomware attacks. Firewalls scan the traffic coming from both sides, examining it for malware and other threats. With endpoint protection, individual endpoints are shielded from threats. There are certain types of traffic that are more prone to carrying threats, and endpoint protection can keep your device from engaging with those kinds of data.

\*Only Download from Trusted Sites

* If you are not familiar with the site or if its Uniform Resource Locator (URL) looks suspicious even though it appears to be a trusted site, you should steer clear. Always double-check the URL of a site before downloading anything from it.

\*Keep Backups of Important Data

* If your data is backed up to a device or location you do not need your computer to access, you can simply restore the data you need if an attack is successful. It is important to make sure you back up all critical data frequently because if enough time goes by, the data you have may be insufficient to support your business’s continuity.

\*Use VPN when using Public Wi-Fi

* A VPN encrypts the data flowing to and from your device while you are connected to the internet. In effect, a VPN forms a “tunnel” that your data passes through. To enter the tunnel, a user has to have an encryption key. Also, to read data that goes through the tunnel, a hacker would need to decrypt it. To block ransomware, a VPN keeps outsiders from sneaking into your connection and placing malware in your path or on your computer.

\*Use Security Software

* Security software uses the profiles of known threats and malicious file types to figure out which ones may be dangerous for your computer. To stay current, security software often comes with free regular updates. As long as you make sure your software is updated periodically, you will have the best protection the software can provide.

\*Do Not Use Unfamiliar USB Device

* A Universal Serial Bus (USB) device can be used to store a malicious file that could contain ransomware. If you ever find a USB device, do not insert it into your computer. The safest USBs are those purchased from a store and sealed inside intact packaging.

\*Avoid Giving Out Personal Data

* If you avoid giving out personal data, you make it far more difficult for an attacker to levy this kind of attack, particularly because they would have to find another way to figure out your passwords or other account information. Personal data also includes the names of people, pets, or places that you use as the answers to security questions for your accounts.

Advanced Persistent Threats (APTs): APTs are sophisticated malware that can evade detection and remain undetected for long periods. They are often used in targeted attacks on high-value targets such as government agencies and businesses.

PREVENTIONS:

\*Email Filtering

* During email filtering, the software automatically moves unwanted emails to a separate folder after analyzing them for red flags that signal phishing.

\*Endpoint Protection

* Endpoint protection platforms examine files as they enter the network. With endpoint security, you'll not only be protected from malicious software, you'll also be protected against evolving zero-day threats.

\*Access Control

* Providing access to and using company information and resources is a fundamental component of data security. By authenticating and authorizing users, access control policies ensure they have access to company data in accordance with their claims.

\*Monitoring of traffic, user and entity behavior

* Monitoring network events generated each day by users, users, and entities is the process of gathering insight into their behavior. By collecting and analyzing this data, you can identify compromised credentials, lateral movement, and other malicious activity.

Botnets: Botnets can be used to launch large-scale attacks such as distributed denial of service (DDoS) attacks or to steal sensitive information such as login credentials or financial data.

PREVENTIONS:

\*Install a Windows Firewalls

* Though sometimes tempting for end users to disable, a properly configured Windows firewall can block many network-based exploits. This measure is especially appropriate for large agencies with many similarly configured machines.

\*Disable AutoRun

* The autorun feature, which automatically installs software, should be disabled to prevent operating systems from blindly launching commands from foreign sources.

\*Break Password Trust

* Judicious control over local accounts, especially the local administrator account, is critical to isolating and eliminating threats. Disabling computers’ capability to automatically connect to each other closes the path that botnets take to spread to the internal network. This is particularly critical in environments were machines store highly confidential data.

\*Consider Network Compartmentalization

* IT managers should establish private virtual local area networks (VLANs), or access control lists (ACLs) between subnetworks to limit exposure. This strategy is not a good fit, however, in environments that mix voice and data communications, as it tends to break the ability to negotiate virtual circuits on the fly.

\*Provide Least Privilege

* Preventing users from being administrators also makes it more difficult for their user account credentials to spread malware, should the computer become infected.

\*Install Host-Based Intrusion Prevention

* This approach does not fix technical flaws or holes in operating systems or application software, but it can reduce the chances that exploits will be successful. These tools are highly effective, but they are expensive and challenging to deploy.

\*Enhance Monitoring

* Around-the clock monitoring is ideal, using products that collect data on network traffic, train devices to monitor abnormalities, and detect and prevent intrusions.

\*Filter Data Leaving the Network

* To stop these communications, and the threats associated with them, agencies can prohibit unwanted traffic from leaving the network, a tool known as egress filtering. Agencies should force Internet traffic through proxies or content filters (see below), or deploy a data loss prevention (DLP) solution.

\*Use a Proxy Server

* While it is impractical to block all potentially hostile outbound traffic, forcing outbound traffic through a proxy server gives agencies a secondary choke point for monitoring and controlling Web access and for defeating some attempts to tunnel around security measures. Content filtering is appropriate for almost any agency.

\*Install Reputation-Based Filtering

* Tools like IronPort and WebSense can help block e-mail from, and requests to, addresses that have reputations as potential malware sources.

\*Monitor DNS Queries

* The way that a workstation responds to domain name system (DNS) queries is often an early warning sign that the workstation may be infected. Specifically, responses from workstations that contain very low time-to-live (TTL) values should be monitored, as low TTL can indicate infection. Monitoring allows system administrators to act before the infection spreads too far

Rootkits: Rootkits are designed to hide their presence on a victim's computer and can give attackers complete control over the system, allowing them to steal sensitive information or launch attacks.

PREVENTIONS:

\*Phishing Awareness

* It is therefore vital for end-users to be aware of common phishing attack tactics, always check a sender’s email address, and never follow links directly from email messages.

\*Software Updates

* Updating software at all times and ensuring it is set to automatically update is one of the best defenses against rootkits.

\*Use Antivirus Solutions

* Antivirus software alone is not a solid defense against cyberattacks. However, antivirus systems as part of an overarching security solution are integral to the fight against malware and help users discover the presence of rootkits.

\*Scan and Filter Network Traffic

* In addition to antivirus systems, use traffic filtering software to monitor and scan the traffic coming in and out of networks at all times. This software scans inbound and outbound traffic to detect malware before it can infiltrate machines.

Fileless malware: Fileless malware can operate entirely in memory, making it challenging to detect and remove. It can be used for a range of malicious purposes, including stealing data or launching attacks.

PREVENTIONS:

* Disable PowerShell and WMI if you’re not using them.
* Disable macros if you’re not using them. If you are, digitally sign and use only those vetted specifically for the company. No signature means don’t use it!
* Regularly check security logs for inordinate amounts of data LEAVING the network.
* Look for changes in the system’s usual behavior patterns when compared against baselines.
* Update your software regularly.