BEST PRACTICES FOR WORK AND HOME DATA PROTECTION

Cyber attacks are on the rise. The tactics of hackers are becoming more and more advanced as these cyber criminals continually hone their “craft.” Your business and personal data are their target so you must protect yourself from predation.

The good news is that there are some straightforward steps you can take. This guide provides a few of the industry-standard best practices for protecting your business and yourself from being the victim of a cyber crime.

INDUSTRY BEST PRACTICES INCLUDE:

- **Antivirus Software**
- **Password Management**
- **Two-Factor Authentication**
- **General Software Updates and Patches**

ANTIVIRUS SOFTWARE

Antivirus software can protect your system from phishing attacks, viruses, worms, spyware, Trojans, ransomware, and Zero-day attacks, to name a few. The number of different antiviral solutions available has become staggering. To mitigate the overwhelming task of choosing which is best for you, here are the most important features you want to include in the program you select:

VIRUS AND MALWARE DETECTION

Detecting and removing viruses and malware is the primary function of any antiviral solution. Programs typically scan files on your computer and compare data in the files to a database of known signatures. Databases are updated regularly to ensure your program has the most up-to-date signatures to detect all known threats. Your program should include both on-access and on-demand scanning. On-access scans files in real-time when they are opened, saved, and run for immediate threat detection. On-demand scanning is performed manually when you want to select the drives and folders you need scanned.

SYSTEM ANALYSIS AND FILE QUARANTINE

System analysis involves monitoring your computer for signs that system components are not functioning correctly. This may be an indication that your system has been infected even if a virus is not detected. When a system problem is recognized, the program can initiate a scan to detect the cause. If a virus is detected, the infected file will be quarantined. Placing a file in quarantine instead of automatically deleting it, is an important feature that helps protect your computer against false positives. The detected file is cut off from system resources. This allows you to have the option of removing it from quarantine if the file is deemed safe.

MALICIOUS URL BLOCKING

A malicious URL is a clickable link that directs users to a malicious or otherwise fraudulent web page or website. By simply clicking on a malicious URL, you may find yourself the target of a phishing attack, have malware auto-install onto your device, or have something more sinister occur. When your antivirus software includes malicious URL blocking, a website is blocked as soon as the program detects malware.

EXPLOIT PROTECTION

An exploit is a piece of software, chunk of data, or sequence of code that triggers a vulnerability that allows the attacker to run a shellcode. The shellcode runs special instructions called a payload which then executes a malicious action. Where web filters, intrusion detection, and other technologies require previous knowledge of a specific malicious code, effective exploit protection shields popular applications and browsers from attack with advanced security. When a shielded application is being exploited, the program automatically stops the malicious code from executing.

EMAIL/PHISHING PROTECTION

Email/Phishing Protection stops spam and malware with inbound filtering. Each email is filtered and sanitized before it is delivered to your mail server. This protects you from email threats using virus scanning, spam scoring, real-time intent analysis, URL link protection, and reputation checks. Programs also include outbound filtering which stops attacks originating from inside your network. This protects your partners and customers, as well as keeping you and your business from being added to spam block lists.

BEHAVIOR-BASED PROTECTION

With the fast-paced evolution of cyber crime, new methods of combat have been required to keep ahead of hackers. Behavior-based protection programs proactively approach security by monitoring all relevant traffic to identify and deal with deviations from normal behavior patterns so that they can be identified and dealt with quickly. Where signature-based tools are best at identifying and repelling known threats, behavior-based programs are necessary for fighting zero-day exploits that have yet to make it onto a malware database.

PASSWORD MANAGEMENT

Passwords are the first line of defense against cyber attack, so having strong, and unique passwords are really important. However, most people tend to reuse passwords on multiple sites. This means that if your password is compromised on one site, hackers can easily use it to get into your other accounts as well. Simply put, coming up with different, high-strength passwords, and remembering them for all of the accounts that you have, is just plain difficult. That is where a password management application comes in.

Password management apps are secure, automated, all-digital replacements for that spreadsheet or notepad where you have jotted down your numerous passwords. The software also auto-generates highly secure passwords that are totally random, and therefore, much more difficult to hack. All you need to remember is one master password and the manager will remember everything else. In many cases, credit card numbers, addresses, bank accounts, and other information is also stored for you. It is advisable to keep that master password written down on a physical piece of paper and keep it somewhere safe and secure.

Once you start using a password management app, you will wonder how you ever survived without it. Ease of use and security on your end, but a huge obstacle to cybercriminals.

TWO-FACTOR AUTHENTICATION (2FA)

An additional layer of security added into the log-in process, Two-Factor Authentication, also known as 2FA, helps verify your identity and protect sensitive login and password data from being hacked. 2FA usually comes as a One Time PIN (OTP) sent via SMS text message or an authenticator app, a fingerprint scan, facial recognition, or a security question. Even if your password has been compromised, adding 2FA into your security toolbelt is very effective in protecting against cyber attacks. Most cyber criminals do not target specific people. They target easy prey with weak security. If one person's data proves difficult to hack, they will move on to someone less protected. That's why 2FA keeps you safe in most instances.

GENERAL SOFTWARE UPDATES AND PATCHES

Software updates are more important to your cyber security than you may think. They not only add new features and improve existing ones, they patch security holes. So, don't be tempted to click on the "Remind me later" button when those little pop-up windows appear on your computer, laptop, tablet, or mobile device. Software updates patch flaws by repairing security holes or fixing or removing computer bugs. When you do not update the software, you essentially leave an open door making you vulnerable to savvy hackers who create malware specifically targeting those holes. Being hacked can also mean that you spread the virus to your business associates, customers, family, and friends. The most simple solution to avoid the pop-ups? Configure your devices to update automatically.

PREVENTION IS KEY

"Intellectuals solve problems, geniuses prevent them."
~Albert Einstein

There are so many programs available on the marketplace that help prevent you from becoming a victim of cyber crime. Be a genius, not a casualty in the war against hackers by taking the time to understand your risks and implementing these relatively simple best practices.

TIME IS OF THE ESSENCE

We get how busy you are and how valuable your time is. You didn't start your business just so you could spend time fighting off cyber attacks. That's where we come in. FUSE3 has over 20 years of experience and we know only too well how technical issues can lead to a loss of productivity and profit, and how technology will help you achieve more. Contact us for more information on how we manage security and disaster recovery planning. We work to keep your business running smoothly so you can focus on what you do best.

CONTACT US TODAY

FUSETHREE.COM | FUSE3