Windows Security Tips

In addition to cellphones, laptop and desktop computers are typical repositories of highly personal and private information. Due to the large Microsoft Windows user base, it is a platform often targeted by hackers, viruses, trojans, malware, and spyware. Presented here are a few steps you can take to protect your computer and data.

ENABLE ENCRYPTION ON YOUR PC

First introduced in Windows Vista, BitLocker encryption helps safeguard information stored on your computer. BitLocker is included by default but not enabled on many Windows computers, and it is more trouble than it should be to turn on sometimes. Regardless, we highly recommend that you enabled this feature, especially on a laptop computer that could easily be stolen. Be sure to hide your recovery key away in a secure place such as a safe and not in the briefcase where you keep your laptop.

USE STRONG PASSWORDS

It is important to utilize a strong password for your Windows user account and your email. The integrity of your encrypted volume is only as good as your account password. Using a strong and unique email password is critical because if this account is breached, a password reset can be conducted on your other accounts and anyone with access to the email can then access those accounts as well. Access to someone's email is like having the master-key to the kingdom, unless two-factor authentication is in place for other accounts. We highly recommend enabling two-factor authentication whenever available.

You will also want to set the screensaver to turn on after a short period, and require authentication after halting the screensaver. The location of these features varies by the version of Windows.

USE A FIREWALL FOR TRAFFIC IN/OUT

Windows includes a built-in software firewall that you should enable, but it does not include much in the way of controlling outbound traffic. For this purpose we recommended the ZoneAlarm program. ZoneAlarm notifies you of whatever application/process is attempting to send traffic out from your computer. By monitoring ZoneAlarm's alerts, you can deny threatening or unnecessary communication to third-party servers. Without outbound protection, the contents of your entire hard drive could be uploaded to another party in a matter or hours.

If you are a business, you should also consider a hardware firewall option. These generally require professional configuration and maintenance. Another even more advanced supplement to a hardware firewall is an intrusion detection system (IDS). An IDS actively monitors traffic on the network and alerts information security personnel if anything unusual is occurring, allowing them to respond before even more damage is done.

COVER YOUR CAMERA

Consider using a small sticker to cover your computer's webcam when it is not in use. If your computer is remotely compromised this will prevent the attacker from monitoring whatever is going on within view.

Unfortunately, microphones are much more difficult to disable, so if you are concerned that your computer may have a virus or spyware infection know that someone could potentially be listening in on you.

MINIMIZE USE OF CLOUD STORAGE

We recommend generally limiting the information you store in the cloud. When storing your data on a cloud server, it is connected to the internet 24 hours a day, 365 days a year. In the event that the cloud provider's servers are breached, your data could be compromised. Think of storing information in the cloud just the same as storing information on someone else's computer. Would you trust someone else to protect your most sensitive data?

If you do use cloud storage, consider encrypting the data independent of the default option offered by the cloud provider. For example in Microsoft OneNote, individual tabs can be protected. When this is done, additional encryption is added, increasing, but not perfecting security. Other independent encryption options are available for ZIP and PDF files.

SECURELY BACKUP YOUR COMPUTER

If your computer is stolen, the hard disk fails, or you forget your password, you'll want to have a backup. Backups should be regular, but introduce a new vulnerability. If you don't encrypt the backup disk and it is stolen it's just as if your computer itself went missing. Using Window's built in Windows Backup feature you can choose what to back up, and then enable encryption for the volume with BitLocker. We suggest using a backup disk that can be unplugged from the computer and stored in a fire/theft resistant safe when not in use. Imagine if you are on vacation and your home or office burns down, destroying both your computer and backup disk.

UPDATE SOFTWARE OFTEN

You'll want to update your version of Windows regularly. Many updates include security fixes that prevent your computer from local or remote compromise. We recommending enabling automatic updates to ensure you don't get too far behind.

Your computer's operating system isn't the only software that needs regular updating. Any other software on your computer can potentially open backdoors into your system. Web browsers are especially vulnerable, and you should keep them constantly up to date. We also recommend avoiding Microsoft's included web browsers and consider an alternative such as Mozilla Firefox.

REDUCE ATTACK SURFACE - NO FLASH, NO JAVA

There are numerous ways that a computer can be compromised. Best practice to lower your risk is to reduce something called "attack surface". This essentially means closing vulnerabilities, and making yourself a more difficult target. Two

major vulnerabilities that exist on many systems are the presence of the Flash Player and Java (not to be confused with JavaScript). Both applications are historically known for poor security. Most users do not need either one of these applications and it is recommended to uninstall them if they are present.

You should also turn off file sharing and Bluetooth unless it is required by your a wireless keyboard of mouse.

DON'T RUN AS ADMIN

Most of us don't plan to get a virus, but it still happens. If you use one account as your administrative account, and another lower privileged account for your daily activities, you make it more difficult for a virus to fully control your system. The only downside to this method is that you will have to type the admin account's username and password more often to authenticate when executing certain system-level tasks.

BEWARE OF MALWARE IN DISGUISE

Websites are able to determine what operating system you are using and present targeted ads. These ads may appear to be local operating system pop-ups claiming that your system has been compromised or needs a "tune up". If you download and install this malware in disguise your system may begin to experience all sorts of issues. If you do mistakenly download malware or spyware, we recommend Malwarebytes Anti-Malware as a cleanup tool.

BEWARE OF EMAIL PHISHING & ATTACHMENTS

A common way computer users are compromised is through email. Sometimes they are sent nefarious attachments which they open and become infected, but in an increasingly common type of attack, they are phished. Phishing is where a malicious actor sends an email that looks like it is coming from a reputable service provider such as FaceBook or a bank. In the email the recipient is informed that they must click a link and enter their username and password for a seemingly legitimate and urgent reason. For example, the email will state that the user's account has been compromised and they must log in immediately to rectify the issue. When they log in, their credentials are sent to the attacker, and the user's

account is now compromised. The attacker often uses this initial attack as a springboard for a broader one. The following are some signs that an email may not be legitimate:

- *ANY* request for you to click a link in your email and enter your username/password or provide banking/credit card information
- Hovering over links show that they go to a site not associated with the alleged service provider, or the domain name seems abnormal
- Variations of a familiar web address (e.g. FaceBoook.com, City8ank.com, twitter.FB500.com)
- Poor use of the English/local language (many phishing attacks are conducted by foreigners residing in countries where they are less likely to be successfully prosecuted if caught)

CONSIDER ENCRYPTED COMMUNICATION OPTIONS

Ensure your home and office networks are either wired or encrypted with WPA2. The original WPA is decent, but if you are using WEP encryption or nothing at all, your network is vulnerable to abuse.

You may also want to consider a virtual private network (VPN). Deployed properly, a VPN can help protect your identify when browsing from home or work and boost the confidentiality of your communications while on public wifi networks.

ANTI-VIRUS & OTHER CONSIDERATIONS

As a Windows user, you must strongly consider installing an anti-virus application. Viruses are highly prevalent on Windows and running without protection is risky. There are many anti-virus options available, but we recommended ESET for home users and CylancePROTECT for enterprise.

Beyond the above, there are additional ways to make your PC more secure, but they are generally more complex or costly. We suggest starting by implementing

most or all of the steps we outlined. If you need additional support, contact us for a personal or business security consultation.