September 2016

TechTidbit.com

brought to you by Tech Experts

Five Tips For Staying Ahead Of Malware

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Malicious software has become an every-day issue for many computer users, and it can have serious implications for your finances. To keep your information, data, and finances safe, you need to be aware of the common threats to your online security that exist and how you can protect yourself against fraudulent activity.

According to research from Kaspersky Security, malicious software, which is also commonly referred to as malware, impacted as many as 34.2% of computer users in 2015. But what is malware and how does it work?

Malware is somewhat different than computer viruses because instead of completely stopping your computer from operating, it sits quietly in your system stealing important and sensitive information.

It is estimated that over 1 million new forms of malware are released on a daily basis in the form of spyware, Trojan horses, phishing links, and ransomware.

Malware is a major issue for both businesses and consumers alike. Although major organizations are investing big bucks in systems that can outsmart the latest malware releases, you also play an important role in preventing malware from spreading.

Here are five actions you can take to do your bit and prevent malware from becoming more of an issue while also protecting your own data and information.

Purchase reliable security software

It doesn't matter how hard cyber security experts work if you don't buy, install and update the software.

Ensure your software is regularly updated

It is imperative that you update all the software that operates on your system on a regular basis.

The majority of malware that is doing the rounds is currently spread online via the Internet; as such, you should regularly update your browser software to ensure you have the latest security fixes and patches.

Be wary of attachments

If you receive emails from anyone you don't know or recognize, do not open the accompanying attachments or embedded links because there's a high chance that they will contain some form of malware.

In fact, if you're not expecting an attachment from the sender, the safest thing to do is call and verify the authenticity of the attachment.

Secure your network

If you use Wi-Fi in your home or business, ensure you secure the network with a robust password. If you do use an unsecured network while at a coffee shop or mall, do not make online purchases or perform any online banking activities.

Avoid clicking on pop-up windows

If you're browsing the web and are presented with an offer of a free scan for malware, don't click on it. There's a high chance that it contains the exact thing you are hoping to scan for. Always scan your computer using security software that you have purchased from a reputable provider.

Malware is somewhat different than computer viruses because instead of completely stopping your computer from operating, it sits quietly in your system stealing important and sensitive information.

Drawbacks To The "Smart" World

"Even if your smart devices don't store information vital to you, they can still act as a gateway to anything else on your network."

We have mentioned ransomware and viruses many times. It's something that can be seen daily without much effort. Everywhere you look, a computer is hacked and held for ransom. The user ends up losing everything in most scenarios.

However, in today's world, we have more than just laptops and desktops. What if someone hacked your fancy new "smart" device? If someone took over or locked you out of your phone, then what would be your next move? What if they locked your home devices like your thermostat or refrigerator? The technological world can sometimes cause quite a panic.

The first question to address is a pretty big concern: How in the world does this even happen? With poor security standards, it's not the most difficult job for those with malicious intent. In the most recent scenario released, a thermostat was hacked by adding files remotely and setting them to run in the background.

The operating system on the device did not check the security or contents of any files processed and ran the ransomware, which then requested money. In this case, if the victim did not pay, the temperature would be locked at 99F degrees.

Sadly, this is just one example. While not all malware attacks on smart devices may cause this type of concern, others are no better. Some other attacks will actually store data on the infected devices, then perform DDOS attacks against unsuspecting victims.

Small apps and programs that can be used for phishing can also find their way onto devices and be completely unknown to the user.

Fixes have rolled out over time for some of the bigger concerns, but there always seems to be something new. With these on your network, it's not a big step to get to your actual files and programs on your PC either.

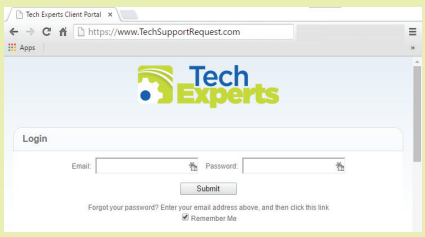
Currently, not everyone has a smart appliance in their home. That said, smart phones have obviously worked their way to the larger majority. We all download apps for one reason or another to make the phone better serve us. A wave of people will flock to the latest craze and download the most popular apps. In these scenarios, there are often "fakes" as well. These will offer some form of related service or product but will also bundle in malicious code. This code has all sorts of capabilities. Some may send texts without the owner's knowledge. Other times, it's possible to have information stolen. The possibilities are sometimes frightening.

So what can be done in the world of smart devices encroaching on all sides of life? In terms of larger devices and appliances, there isn't room for removal and clean-up on the user side.

Developers are both the ones at fault and the ones that will find solutions ahead of time for the worst infections and hacks. Phones can have anti-malware programs run to help prevent data breaches, however. Most will come with a manufacturer version, but it's always best to explore options to ensure you are protected.

Even if your smart devices don't store information vital to you, they can still act as a gateway to anything else on your network.

As such, your office area or business workstation may fall victim soon after. Since these are the real powerhouses that hold your programs, data, and backups of other devices, it's imperative to keep these clean and functional. Luckily, there are teams such as the one at Tech Experts that are able to identify and neutralize a threat. That alone adds peace of mind in a sometimes uncertain "smart" world.



Create new service requests, check ticket status, and review invoices in our client portal:

http://TechSupportRequest.com

Should Your Small Business Use A Domain Network?

Luke Gruden is a Help Desk Specialist at Tech Experts.

If you have 5 or more computers that are sharing files and are constantly being worked with, a domain network would be in your best interest.

A domain network using a server has many benefits to a work area, a work building, or even multiple buildings using VPN. The flexibility, security, and convenience of a domain is, in most companies, invaluable. Sign into your account from any computer that is a part of the domain and you no longer need to use only your personal computer to access files.

If something were to happen to your computer, you could just use another computer to sign into your account and continue working without much downtime. This is also a far more secure way for users to access other computers as they have to use their credentials and only have the permissions that their credentials provide, not those of the computer itself. As long as users are not sharing passwords, you can have every user accounted for, policies implemented, and control what they can and cannot access when it comes to Internet, files, and programs.

Secure file-sharing is an easy and basic function of a domain server with Active Directory, which all the computers connected to the domain have access to. If you wanted only certain users to have access to certain files, you can have folders set up that prevent unauthorized editing, but still could be read — or even not be seen at all.

Having 5+ workers able to access the same set of files to edit as needed is an amazing way to save time and improve project efficiency. Everyone can see the file as it is saved or changed and they can continue to edit records as necessary without ever having to go on the Internet or transfer the file. Just get on any computer on the domain and you have instant access to the files that you need without a second thought.

Active Directory is your IT department's best friend when it comes to handling large or small groups of computers as IT can access the domain server to make adjustments to other computers without ever stopping the work flow.

Forgot your password? Your IT can very easily use the server and reset your password for you without having to go to your computer. Setting up a new computer that needs certain printers and drivers installed? IT can set up the server to push those standard programs and drivers without having to install each individual program. Need to set up a new user account? It's created on the server and the user can be accessed on all computers. There are so many possibilities that open up when you have a server domain available for your workstations.

We have only scratched the surface of what's possible with a domain server and the amount of time and effort it can save for everyone in the company. I believe every business that is looking to grow should have a domain server early on as it will be easier to set up and can evolve to your needs as your company grows.

If your company needs help setting up a domain network, you can count on Tech Experts to take care of it.

"The flexibility, security, and convenience of a domain is, in most companies, invaluable. Sign into your account from any computer that is a part of the domain and you no longer need to use only your personal computer to access files."

Four Ways To Avoid Prolonged Sitting At Work

Prolonged sitting at work is a global problem that is unlikely to improve any time soon. So what can you do to incorporate movement into a sedentary job to reduce the damaging effects prolonged periods of sitting will have on your health?

Use a standing workstation. It may not sound particularly comfortable, but standing at your desk for some periods during the day will reduce the negative consequences of desk work. Invest in a decent stand-sit workdesk solution so that you can switch between standing and sitting in accordance with your comfort needs.

Stand while talking. If you don't want to go all in andwork in a standing position, make sure you take regular breaks from sitting. One way of achieving this could be to stand every time you are talking on the phone. You may also wish to stand while working on brainstorming activities or while engaged in group workshops.

Stretch regularly. According to the experts, it can be unhealthy to remain in a single posture for more than 30 minutes. If you feel your muscles tightening, stand up and give your body a stretch. The Mayo Clinic has published a handy guide to office stretches that workers can complete while engaged in other tasks.

Get your posture right. Complete a workplace assessment to test the extent to which your seating and working position are ergonomic. Identify any areas of weakness and make the appropriate changes, such as repositioning your monitor, immediately.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

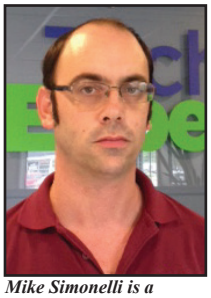
Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Why It's Important To Change Your Router's Default Log-in



Mike Simonelli is a Senior Network Technician at Tech Experts

It's a pretty common scenario: a small business wishes to add Wi-Fi to its existing network infrastructure. A quick trip to the nearest big-box store reveals several Wi-Fi capable routers or access points to choose from. Grabbing up the mid-priced model, the business owner heads back to the shop and uses the included Ethernet cable to plug the new device into an existing switch and, just like that, instant Wi-Fi.

There are a couple of concerns regarding the above scenario that the savvy business owner should be having. The first and most obvious: "I plugged it in and now everyone with a laptop has unrestricted access to my network." How do you control who can connect to your Wi-Fi?

The answer is to enable a wireless security protocol on the router or access point. WEP is an acronym for Wired Equivalent Privacy (or Wireless Encryption Protocol) and it was designed to provide the same level of security as that of a hard-wired Ethernet connection.

Because wireless networks broadcast messages using radio waves, they are subject to eavesdropping. WEP provides security by encrypting the data to protect it as it is transmitted from one point to another. Almost all wireless devices will support WEP and instructions for enabling it on a particular device should be readily found in the documentation.

Enabling WEP will keep people without the correct password off your Wi-Fi and also prevent unauthorized eavesdropping of network traffic.

Another often overlooked concern is changing the default credentials that are needed to login and administer the new wireless device.

I can't tell you how many times that I've connected to a wireless network and browsed to the default gateway I was assigned (normally something like http://192.168.0.1) and typed in "admin" and "password" on the login form that is presented and gained access to the router's configuration.

The username "Admin" and the password "password" are typically the default credentials as they come pre-configured on Linksys routers, as well as some other brands.

If these credentials work, then potentially anyone can have unrestricted access to your router's configuration. At this point, no wireless security protocol such as WEP will protect you since it can simply be turned off in the router's administration interface.

Worse yet, an intruder can set his/her own password and change the admin password to something else. Once this happens, usually the only way to regain access to your own Wi-Fi network is to factory reset the device, which removes all of your configurations.

The bottom line - never leave a wireless device at its default settings when you connect it to your network. By taking the time to follow these simple guidelines, you will make your wireless device a worthwhile addition to your infrastructure, as well as making your network that much more secure.

If you have any questions during your router set-up or if you'd like to find out how to increase your office's security using your current router, give Tech Experts a call at (734) 457-5000, or email support@mytechexperts.com. We'd be happy to help.

Create new service requests, check ticket status, and review invoices in our client portal: *http://www.TechSupportRequest.com*