November 2011

TechTidbit.com

brought to you by Tech Experts

For Small Businesses, Smartphone Security Is As Important As PC Security

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

Although there aren't any prevalent security attacks or threat mechanisms associated with smartphones in the market today, security vendors and analysts are urging mobile device users to use security best practices on them, just as they would with their computers.

With recent advancements around mobile devices and technologies, particularly smartphone devices, more and more people are staying connected both in the home and office environments.

Analysts at Forrester Research, a leading authority on security in the small business IT space, say the new breed of smartphones, such as Android and iPhone-based devices, are built on operating systems that are "fairly-well locked down."

However, although they said using these types of devices are generally safer than PCs because malware can't run on them (yet), there are still privacy and data risks to be aware of.

GPS hacking is just one concern - a rogue phone application sending your location to an outside service without your permission.

Privacy-related issues will emerge as third-party "fake" applications access more of your personal data.

These would be apps that look legitimate, but are designed to steal your personal information.

Fixing this type of issue will be simpler than a PC, though: The operators of the "app stores," (Apple and Google) can find the offenders and remove them from the sites in a matter of minutes.

Security and privacy are a concern especially for users who bring and work with their personal devices in and out of the workplace.

The safety of the data on those devices becomes an even larger issue.

Smartphones allow business owners and employees to be more connected with each other. Users are sending information via e-mails and through attachments, all of which are susceptible to loss or theft.

Smartphones that are used for business communication should be treated like office PCs when it comes to data protection. The security threat is there - you have to protect the data that's on the device.

One of the biggest security mistakes customers make with their mobile devices today is that they fail to use even the most basic security protection methods such as passwords.

Most users don't set up passwords on their mobile device because they think of their smartphone as just a phone.

But really, it's a small, low-power computer that happens to let you make phone calls, too.

For small business, it's time to start thinking of smartphones as another entry into your business' data. If they're used for business communication, they need to be monitored, protected and updated just like a PC on your network that attaches to your server and financial data.

Happy Thanksgiving!

Industry Standard Security Best Practices

Network security is a must in any network, but when it comes to a business network, there are a number of security standards and best practices that ensure you have control over your network.

Businesses in certain industries secure. Many different companies require different security standards; one organization for instance is the PCI (Payment Card Industry). The payment card industry has very a strict network security standard.

The below practices are fairly strict and will offer you a great deal of control and protection against data theft and network intrusion.

Modem

We will start from the outside edge of your connection of your network and work our way in from your modem on into client workstations.

The modem is probably the simplest device on the network - you can't really secure it (beyond performing regular updates), but some ISP's feature a built in firewall in the modem. This can be turned on or off to work in conjunction with your company's firewall.

Firewall

The next item to take a look at is your router/firewall. Generally you would have a router that offers several ports you can connect to via a direct Ethernet connection as well as WiFi access.

This firewall will add another layer of protection for when your network connects to the Internet. When configured properly, you would block all unauthorized network connections. As far as protecting the WiFi goes you are best to enable MAC filtering.

Each piece of network hardware has a unique identifying numerical code, called a MAC address. Filtering by MAC lets you set up WiFi so that only devices you explicitly define are allowed to connect to your network.

Once you have MAC filtering in place, you can also encrypt network traffic and use a long secure password. Since the clients on the network will not need to type this password in all the time, it is best to make a complex password containing both capital and lower case letters, numbers, and symbols.

Another option to further increase security when it comes to WiFi connections is to set the access point to not broadcast it's SSID. This will make it look to the normal person as if there is no wireless connection available.

Server

There are a lot of features that can be enabled at the server to further improve network security. The first item to review is the group policy. Group policy is part of the server operating systems that allows you to centrally manage what your client workstations have access to and how.

Group policies can be created to allow or deny access to various locations on your users' desktops. You can get as granular as defining a group policy that sets standards on user passwords.

By default, Windows Server 2008's password policy requires users to have passwords with a minimum of 6 characters and meet certain complexity requirements.

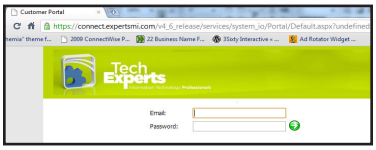
While these settings are the defaults, generally 8-10 characters is recommended as well as mixing upper and lower case letters, numbers, and special symbols. An example of a complex password might be @fF1n!ty (Affinity). This password would meet all complexity requirements and is fairly easy to remember. Passwords should also be forced to reset every so many days. A good time period is roughly 30 days.

One other possible option is to have firewall software installed on the server itself to regulate traffic in and out of the server.

The nice thing about having a firewall on the server itself is that you have the ability to log failed connections to the server itself as well as what that connections is and where it was coming from.

This feature alone gives you a lot more control over the network. For example if you noticed in the firewall logs on the server that a connection you didn't want getting through was making it to the server you can go back and edit policies on the router/firewall to attempt to

Continued on page 4



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

Backing Up And Restoring Files With Windows 7

In the business world it's critical for end users to have a backup solution available in case of data loss or system failure.

System Restore is one of the easiest ways to restore files and settings. If you can't find a file on your computer or you accidentally modified or deleted a file, you can restore it from a backup if you're using Windows backup in Windows 7, or you can try to restore it from a previous version.

Previous versions

Previous versions are copies of files and folders that Windows automatically saves as part of a restore point. Previous versions are sometimes referred to as shadow copies.

System Restore is a component of Microsoft's Windows Me, Windows XP, Windows Vista and Windows 7 operating systems that allows for the rolling back of system files, registry keys, installed programs, etc., to a previous state in the event of system malfunction or failure. Using System Restore to restore previous versions is simple.

Simply open up any Explorer window, right-click on a file or folder you wish to restore, and select "Restore Previous Versions."

For instance, if you accidentally deleted a file from a folder in My Documents, browse to a file you would like to restore from an earlier point (all of the contents may have been over written mistakenly.)

Likewise if you have accidently deleted a few documents from a folder within your My Documents folder titled "Easter Pictures," simply right-click on the folder and select properties, then select the previews versions tab, then open previous versions from it.

Please note that this will only appear on files and folders, not drives or Libraries in Windows 7.

The dialog will show all of the previous copies of this folder that are available. Click on the time you wish to restore from.

You can choose to either Open, Copy, or Restore the folder. If you click Restore, you can restore the full contents of the folder as it appeared at some time in the past.

Choose "copy" to copy the entire contents of the folder as it appeared at that time to another location. For instance, you could copy it to a flash drive for safe keeping, which also previews overwriting the current file.

Lastly you can choose "open" to browse the contents of the folder as it appeared at that time.

You can open, copy, or do anything you choose with the file from here. For instance, if you deleted a folder named emails accidentally today, you could click copy, and then paste it into the location of your choice.

When in this mode, you are directly browsing the shadow copy of your hard drive. The path to the folder shows the date and time of the copy.

And, the great thing is, this feature is available in all editions of Windows 7, including the low-cost Starter edition often preinstalled in netbooks.

System Restore is a great way to back up your files in case of accidental deletion, or unwanted changes, but should not be used for your disaster-recovery plan.

In cases of disaster-recovery, you will want to make sure you have a proper backup set to automatically backup your systems, System Restore should only be used as an addition to the backups you currently have setup with your IT professional.

Try These Tips To Make Windows Work Better For You

Quick web address
Type the name of a website such as 'google' into your browser's address bar and press CTRL+Enter to automatically add http://www and .com and be taken to the site.

Save a web page picture
To copy a picture from a website on to your computer, right-click the image and select Save Image As or Save Picture As.

Move between web links
Use Tab and Shift+Tab to move between links on a web page and press Enter to follow the selected link.

Change the clock
Double click on the clock on the Taskbar to change the time and date shown.

Create a web shortcut
Right-click on a web page in your browser and select Create Shortcut to place a shortcut link on your desktop.

Take a screen snapshot
Press Print Screen to take a snapshot of the whole screen or ALT and Print Screen for just the current window, then paste it into Microsoft Word if you want to print it, or an an image editor such as Paint to save it as a picture file.

Industry Standard Security Best Practices, Continued From Page 2

further lock down your network from that point as well as blocking it at the server.

One final quick thought on server security is physical security.

Generally it is a good practice to have the server physically locked in a room that only specific people have access to. If you really wanted more control as well you can have the server locked using a system that logs who comes in and out of a room via a digital keypad and their own passwords.

When it comes to your workstations, employees should only be logging into the workstation via their domain login and not using the local admin login.

This will allow you to centrally control via group policy what they can access like stated above. You can also configure roaming profiles so that if someone was to steal a physical workstation they would not have access to any company information as it would all be stored on the server and not that workstation - which is another great reason to have your server locked up.

Employee logins to workstations should also have account lockout policies in place so that if a user attempts to login too many times with an incorrect password, the server would lock them out on that workstation for a time period set by the administrator. One other item you could have in place for various employees is specific time periods their credentials will allow them to log into the systems.

One final step in network security is having good anti-virus software installed on your workstations and your server. A compromised machine can be giving your passwords and information away to hackers making it possible for them to waltz right into your network undetected.

You are best protected by having as many of the above security steps configured and working properly on your network.

Determine what your network needs, evaluate the practice after it has been in place for a month and make the proper adjustments to ensure your network is safe. You should also preform regular security audits.

If you would like to see how secure or unsecure your network is give us a call and we can perform a network security audit for you and let you know where you stand!

Featured Article Written By:
Frank Wright

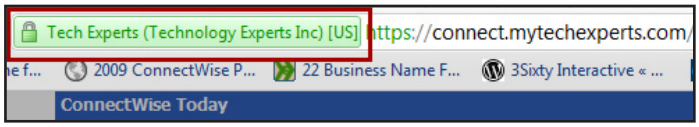
How To Shop Online More Safely And Securely

These tips can help you determine that you're shopping at a secure and trustworthy website.

Look for signs that the business is legitimate. Buy only from reputable stores and sellers. Here are some ways to check.

Find out what other shoppers say. Sites like Epinions.com or BizRate have customer evaluations which can help you determine a company's legitimacy.

Look for third-party seals of approval. Companies can put these seals on their sites if they abide by a set of rigorous standards such as how personal information can be used. Two seals to look for are the Better Business Bureau seal, and the TrustE certified privacy seal. If you see the seals, click them to make sure they link to the organization that created them. Some unscrupulous merchants will put these logos on their websites without permission.



Look for signs that the website protects your data. On the web page where you enter your credit card or other personal information, look for an "s" after http in the web address of that page. This shows that the web page is encrypted. Encryption is a security measure that scrambles data as it traverses the Internet. Also make sure there is a tiny closed padlock in the address bar, or on the lower right corner of the window.

Use a filter that warns you of suspicious websites. Find a filter that warns you of suspicious websites and blocks visits to reported phishing sites. For example, try the SmartScreen Filter included in Internet Explorer.

Keep your web browser updated. It helps protect you when you shop online.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

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

TECH EXPERTS

1206 South Telegraph Road
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com