TechTidbit.com

brought to you by Tech Experts

Almost Every Small Business Can Expect To Get Hacked

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

Juniper Networks recently commissioned a study on small and medium company network security.

The startling result: Over 90% of US companies reported at least one security breach in the last year, with more than half indicating they experienced two or more significant security problems with their networks.

There's a misconception among a lot of small business owners that they're safe from cyber attacks, because small companies offer a smaller payback for hacking efforts.

Small business network security is usually lax

The reality is, security policies and procedures at small companies usually make them an easy and simple target for hackers.

While the payout isn't as large as hacking TJ Maxx, invading a small business' network usually takes a lot less effort, and the business lacks a sophisticated response system.

Why is hacking so easy?

A new technique, called spear phishing, let's hackers target a small group of previously identified people. Somtimes, the attack goes after just a handful of people who work at the same company.

Spear phishing does away with the need for hackers to gain access to your passwords. As more companies start to use social media sites such as FaceBook and Twitter, hackers using spear phishing are finding it easier to "trick" unsuspecting employees into installing crimeware on their company computers. This crimeware let's the criminals access the computer system directly. Once they have access to one machine on your network, it's easy to connect to the others.

Preventing & detecting

Recent attacks have highlighted the growing need for companies to implement network security controls to catch the bulk of socially engineered spear phishing attacks.

They also need to take measures to quickly detect and contain security breaches.

The first thing you'll want to do to protect your business is implement a strong firewall (see Frank's article on page two) that lets you assign security restrictions for users based on the content of websites, and even keywords that might be potentially dangerous.

The next thing to look at is your company's acceptable use policy. This can be as simple as a few pages added to your employee handbook that outlines what is and isn't acceptable behavior on your network.

The final thing to examine is your backup and disaster recovery plan. The hacker's aren't giving up, which means it's time to plan for what comes after a security breach.
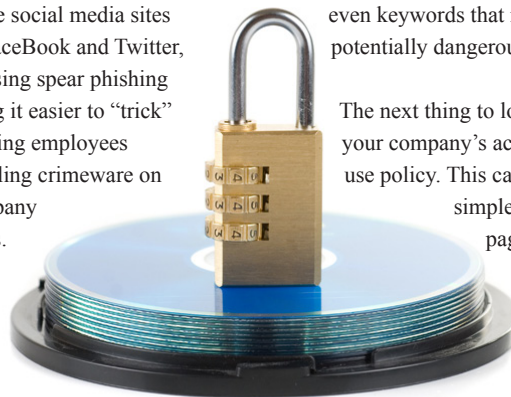
> *"Over 90% of US companies reported at least one security breach in the last year, with more than half indicating they experienced two or more significant security problems with their networks."*

Name:
Tech Experts
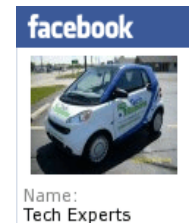
www.MyTechExperts.com/FB

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.

Firewalls: What Do They Do And Why Should You Have One?

Firewalls are network security devices that protect your internal network (your servers and PCs) from your external network (the Internet).

We've put together a basic guide to firewalls - what they are, when you should have one, and why.

What is a firewall?

A firewall is simply a border between the device and the firewall software is installed and running on (and devices on the LAN side of the
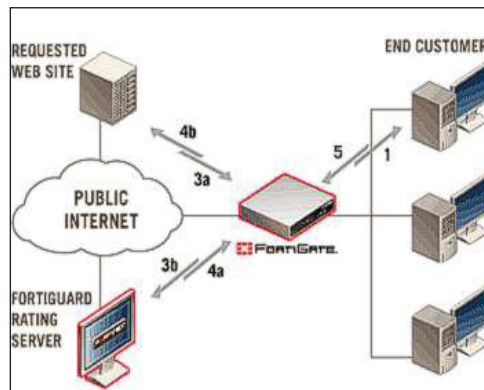
firewall) and any other devices on the outside of it.

For example, there are many different kinds of firewalls. Windows firewall gives you very basic features, and is built into Windows.

This firewall is designed to block unwanted access to the computer itself and is not designed to protect the rest of the devices on a network.

Another form a firewall can take is a separate device all together.

Having a device that specifically functions as a firewall gives more control over what the firewall can be used to protect.

For example it is possible to buy a firewall appliance that can be attached to the perimeter of your network and block specific connections to your LAN.

When is it a good time to look into using a firewall?

On most Windows based computers Windows firewall is generally on by default so most people already run a firewall on their computers without even knowing it.

That being said, Windows firewall does not give you anywhere near the control or protection of a dedicated firewall product.

If your business requires very strict security and data compliance, or you intend to store highly confidential information (an example would be client credit card numbers), it may be in your best interest to have a third party firewall.

Third party firewalls offer much greater protection and allow the ability to configure specific rules in much greater detail than Windows firewall.

Having the ability to configure rules with more detail makes it possible for you to lock down your network and its possible security holes more tightly.

The reason this is a good idea if you are storing confidential information on a network is that having a firewall gives you control over exactly what comes in and out of your network.

Without this added security it may be possible for your valuable information to be compromised or copied to a remote location without you even knowing it is happening.

## Why have a firewall or invest in a better one?

Three words: Vastly improved security. A third party firewall solutions affords you the best protection for your data and network.

If you have important data to secure, a firewall is an excellent step in protecting your network from unwanted access to your network.

If you have questions about your firewall (or lack of firewall) and would like us to evaluate your network ssecurity, please give us a call.

Whether it is security holes left open due to a weak firewall or other possible security issues we can help you secure your data!

Feature article by Frank Wright, Service Manager for Tech Experts
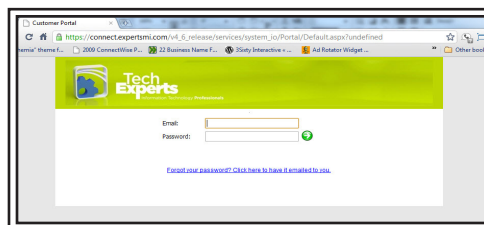
Create new service requests, check ticket status and review invoices in our client portal:

www.TechSupportRequest.com

Improve Your Web Browsing Experience With Add-ons!

There are multiple Internet browser add-ons that can make your web browsing experience more productive and more enjoyable.

Add-ons are programs that are installed into your browser application, which provides additional functionality.

The first Internet browser to introduce is Internet Explorer (IE). IE is one of the most popular web browsers available because it's native to all Windows Operating Systems.

IE has been negatively criticized by many users and technical websites for security issues, but with careful web browsing and the right add-ons Internet Explorer will get the job done.

In the business world there are many websites that requires the use of Internet Explorer.

This limits us from the functionality that we are used to in other Internet browsers like Firefox and Google Chrome.

For example, in Firefox and Google Chrome if you accidently close one of your Internet browsing tabs you can recover it by going to the History option and clicking on recently closed tabs or a key combination of Ctrl+Shift+T. IE doesn't offer this option.

Until Microsoft updates IE, the recommended add-on is called Open Last Closed tab. It is a free download from www.download.

com. Search "Open Last Closed Tab" download and install and you will be satisfied that your Internet tabs are safe from getting closed accidently.

Since it is the most popular browser, Internet Explorer has had more issues with security than most others. It's the most popular, therefore, hackers will get the most "bang for their buck" by attacking IE.

The best way to precent browser security issues to install the add-ons/ toolbars that comes free with the antivirus of your choice.

Phishing is the most common problem. What happens is if you misspell a website or click on a link from an email it will take you to a website that looks similar to the one you are used to.

So when you enter your username and password it actually steals your login information.

A good Choice is Norton's Internet Securities toolbar; all of them will protect you from phishing. However, Norton verifies many popular banking and shopping sites.

One of the best things about Norton is if you see the Antivirus Norton Toolbar display a shield, you know you're dealing with a site that's

been authenticated by Norton as safe and legitimate.

Phishing is the fraudulent practice of sending e-mails that look like they're from legitimate companies to try to get you to reveal personal information, such as credit-card numbers or online banking passwords.

Another very useful browser add-on is Last Pass. Last Pass is an application and add-on that stores all of your saved passwords, login information, and important notes.

For example, if you are in the automotive industry. You will have a number of parts ordering applications and websites to that require passwords.

Last Pass will securely store all of this information and this will also speed up the process when logging in to your software or websites. You can purchase last pass from www. lastpass.com.

Try out a few for yourself. For Internet Explorer add-ons visit http:// www.ieaddons.com/en/.

For Google Chrome add-ons visit https://chrome.google.com/web-store.

And for Firefox add-ons visit https://addons.mozilla.org. There are several thousand add-ons available to choose from.

Feature article by Terrell Canute, Service Technician at Tech Experts

Are You Suffering From Email Overload?
Here's Five Ways To Get Your Inbox Organized, Saving You Time And Frustration

A cluttered and unorganized mailbox can make it difficult to find the email you need. This messy situation can be remedied.

Microsoft Outlook offers great tools that help you sort your email and organize your messages in meaningful, easy-to-control ways. Outlook can even help increase your efficiency and productivity.

Sort messages quickly

Outlook 2010 has a great new feature for organizing messages by date and arranging them by Conversation.

Using this feature, messages that share the same subject appear as Conversations that can be viewed and expanded or collapsed by clicking the icon to the left of the Subject line.

The messages within each Conversation are sorted with the newest message on top. When a new message is received, the entire Conversation moves to the top of your message list.

To turn on Conversations, on the View tab, in the Conversations group, select the Show as Conversations check box.

In all versions of Outlook, you can find messages in mailbox folders more quickly by changing how they're sorted in your email folders. For example, you can arrange your email by date, sender, or file size.

Group similar messages in folders

By creating new mail folders, you can group messages related to each other. For example, you can group messages by topic, project, contact, or other categories that make sense to you. You can even create a folder for all the messages from an important client or vendor.

In Outlook 2010, to create a new folder, on the Folder tab, in the New group, click New Folder. In Outlook 2007 or 2003, on the File menu, point to New and then Folder.

Create search folders to find messages fast

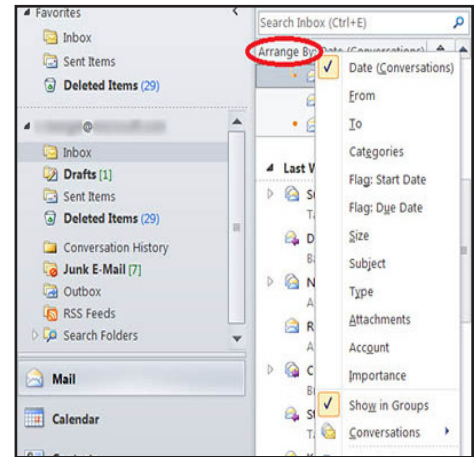Search Folders are a quick way to look at predefined collections of email messages.

They don't actually store any messages themselves. They're virtual folders that offer a view of all the messages in your Inbox that match your search criteria.

You can use Search Folders to help you find all the information related to a particular project, an important client, or an upcoming conference.

To create a Search Folder in Outlook 2010, in Mail, on the Folder tab, in the New group, click New Search Folder. To create a Search Folder in Outlook 2007 or 2003, in Mail, on the File menu, point to New, and then click Search Folder.

Route mail efficiently using mailbox rules

By creating rules for Outlook, you can automatically perform actions on both incoming and outgoing messages based on criteria you establish.

For instance, you can automatically forward all messages sent by your VIP clients to everyone on your sales team, assign the category Sales to all messages you send that have the word "sales" in the Subject line, and more.

Routing mail efficiently not only organizes your mail for you - but also frees up your time from performing routing tasks.

Reduce unwanted email with junk filters

Keep distracting and unwanted messages out of your Inbox by using Outlook Junk Email filters.

These filters send junk email to a separate mail folder in your Inbox.

You can review these messages to ensure that no legitimate messages are there, and if they are, you can adjust the filter to avoid flagging such messages in the future.

It's a good practice to monitor the Junk Email folder to make sure you don't miss any important messages.