Ready Net Go, Inc.

IT Solutions for Businesses ... *Moving Forward*

May 2011

Online Security

If you don't think it can happen to you, think again... Online identity theft and malware attacks are booming right now; no one is immune unless you disconnect entirely. Given the pervasiveness of email, Internet searching, instant chats, texting, and web access via mobile devices, disconnecting isn't an option for most people. So what can you do to protect yourself? We'll go over some advice in this newsletter.

Email and Web

Malware, or malicious software, is the general term for any computer code or script that seeks to disrupt systems (computers and servers). Malware includes viruses, worms, Trojan horses, dialers, and spyware.

It is a huge problem right now since the most common avenue of distribution is through downloaded software over the Internet. In fact, Microsoft considers 1 in 14 files downloaded by users to be malicious. How can this be?

Malware can be bundled secretly with a known program that the user willingly downloads such as a Smartphone application, online game or productivity software such as an anti-spyware application. In these cases, the user downloads the software unaware that there is rogue code included.

Other avenues include clicking a harmful link in an email or on a webpage, even from a search engine's main results page. By clicking the link, software is downloaded without the users knowledge.

In some cases, the malware completely disrupts the system prohibiting any productivity but increasingly, more malware is being created that runs silently in the background, stealing your identity and posing as you to your friends, family and colleagues.

By doing this, hackers obtain personal information; passwords, bank account numbers, credit card numbers, etc. Your accounts can be depleted within moments and then the malware can be sent to other users listed in email or online accounts thereby increasing their reach and potential profits.

Once the process starts, it is very difficult to stop; you may end up consuming many hours cleaning the infection off your computer, resetting passwords and changing account numbers.

So what can you do to prevent this?

Tip of the Month

Microsoft 365

If purchasing software is nowhere on your radar screen these days but you're still interested in using Microsoft Office programs, a monthly subscription-based service may be just the ticket.

Microsoft 365 is similar to Office Web Applications but no initial software purchase is required. Programs included are 2010 Office Web versions of: Word, Excel, PowerPoint, and OneNote, and hosted versions of Exchange, SharePoint and Lync (mobile and desktop application centered on communication tools such as instant messaging, voice, and video).

Microsoft 365 applications can be accessed from any computer online as well as from most mobile devices including Windows Phones, Nokia, Android, iPhone and BlackBerry.

The service was recently released to businesses and soon will be released to the general public. Current rates are $6 per user per month for the first 1-25 users. *See our full review next month.*

Website Worth Watching

► http://www.howstuffworks.com/how-to-tech/how-to-avoid-facebook-scams.htm -

How to Avoid Facebook Scams - If you use Facebook, read this article!

Security Risk Scenarios

The first step in preventing a malware attack or online identity theft is to understand how the attacks happen, then you can choose to engage in an activity or avoid it.

Here are some scenarios that have been known to cause problems for computer users. Above all, be cautious with links you click and software you download. Solutions to these scenarios and more are listed on pages 3 and 4.

1. Online games are notorious for distributing malware especially free games downloaded from peer-to-peer sharing sites like **BitTorrent** and shared on social media sites like **Facebook**. Over sixty million people engage in online gaming making it an easy and lucrative target for thieves.

2. Facebook - This online sharing site has numerous privacy strikes against it, but the biggest problem with Facebook is the lack of control. A message from a friend should be considered safe but oftentimes, people's accounts get hijacked and messages are sent without their knowledge.   We tend to trust those we know and hackers have no problem exploiting this trust.

   Scenario: A well known virus has been circulating around Facebook where an individual receives a message from a friend to watch a video. When you click the link, you are told to download special software in order to watch the video. Since the message came from someone you know, you trust it like every other message you've received from them. If you download this particular piece of software though, your computer becomes infected. Facebook doesn't have many controls in place to determine the authenticity of files, so it's up to each user to determine what they download and from whom.

3. Using the same password for all of your online accounts is a recipe for disaster. Scenario: Let's say someone figures out your email password and what bank you use. If your email and bank account passwords are the same, then the thief not only has access to your email address book (and can send phishing emails to everyone listed inside) but they are now one step closer to cleaning out your bank account.

4. Legitimate programs will not scare you into purchasing their product. Scenario: While browsing some Internet sites all of a sudden you get a pop up box that states you've been infected by a virus and you should download the software to clean your computer. This is classic scareware, software designed to scare you into purchasing bogus programs. The box may have an authentic looking name like Windows Anti-Virus Detector or Internet Defender. The text may state, "If you don't download right now, you will lose all of your data".

5. A common way hackers gain access to your computer is through sending files with multiple extensions. Scenario: You may receive an email attachment with a file such as *text.vbs.exe* or *image.jpg.vbs*. Normal files have one extension such as *file.doc* or *file.jpg*. When you encounter a file with more than one extension it's a good bet that the file is not legitimate and should be avoided.

6. When manufacturers release fixes for their software, oftentimes hackers will create malware to exploit this fix. They hope that people don't update their software regularly and will get infected by their malware. If you want to stay ahead of the game, update your software regularly.

7. Wi-Fi is an Internet connection method for mobile devices such as laptops, cell phones and Internet devices like e-readers and tablets. It's often used in public places to get online for free or used inside the home to eliminate wires.

   The problem with Wi-Fi is that the connection can be easily tapped by individuals within a 120 ft indoor / 300 foot outdoor radius. Scenario: You log onto your local bookstores' free Wi-Fi connection for just a few moments and all of a sudden, your screen is full of pop up messages for Viagra and porn. You've just been hacked by someone nearby and now your computer is infected. You didn't bother using an encrypted connection beacuse it was just going to be a few moments.

Online Security Tips

General Tips

1. Use different passwords for online accounts. Admittedly, it's less convenient to remember multiple passwords but if someone figures out your one password, they have access to all of your information instead of just one part. Information is king; the more someone knows about you, the more damage they can inflict. If you make it hard for thieves, they'll go somewhere else.

2. Make passwords difficult to figure out. If your password can be found in a dictionary, it's not good enough. Likewise, don't use default passwords such as "password", "123", "admin", or easy passwords such as your birthdate or street address. And never, ever use your social security number unless required for some financial or government transactions. Instead, use a mix of letters and numbers and include special characters such as *, ?, % or !. Here's an example of a strong password:

   TRex6#Jun

   What makes this a strong password? It's at least 7 characters, uses a mix of upper and lower-case letters, a number and a special character. You won't find it in a dictionary and it isn't common information attributable to you.

3. Update your software when you get notifications from the manufacturer especially for Adobe Flash. Also install browser updates for Internet Explorer, Firefox, Chrome, Opera, etc. The latest versions are more secure, closing holes or doorways into your computer that have already been exploited by hackers.

   For operating system and productivity software, you'll receive automatic notifications as pop up windows such as Microsoft's Windows Updates or Adobe Flash. For other productivity software like Microsoft Office, you'll have to manually download the updates by going to the website or downloading the updates through the software.

   For free malware detection software, you must install updates from the manufacturer on a regular basis; weekly, if not daily, in order to fully protect your system against the latest threats. Just downloading and installing the program isn't sufficient. If you have trouble remembering, it may be worthwhile to get a paid subscription service.

4. Be suspect of companies, especially large companies, that offer free products. You may be paying for the item or service indirectly through the release of your personal information. Apple and Google, in particular, are being investigated for tracking software that they have included in many of their products. This tracking software constantly monitors your whereabouts and reports this location to those interested in knowing where you are.

Email Tips

1. Stop clicking links in emails, specifically ones that ask you to update your account information. Even if you think it's legitimate, it's not worth the risk. Phony websites are a dime a dozen; company logos and graphics are simple to duplicate and text can be copied and pasted. Instead of clicking the link in the email, type the known address in a browser and bookmark it.

   When you receive an email from the company, use the bookmark link rather than the email link. Most companies know the risks of email security and will not send important information via email.

2. Make sure you're using an email filtering program which automatically filters incoming and outgoing email. These programs flag each message with security levels of low, medium and high according to algorithms (suspect keywords, nonsensical language, inconsistent header data) and allow you to delete the messages before opening.

3. Be suspect of emails that use all caps in the subject line or in the body of the message as well as ones that ask you for money and use bad grammar or have numerous misspelled words; sure signs the email is not legitimate.

Internet Tips

1. Be very selective with the information you share on online social sites like Facebook or Twitter. Don't include personally identifiable information like your address and phone number, or mention when you are going on vacation.

   Take the time to restrict your privacy settings, read the fine print and be suspect of the links you click and download even if it comes from your best friend. No company is immune to hacking and no account is completely secure. Keep in mind that once your information is compromised, it's very difficult to regain.

2. When conducting a search using a search engine like Google, Yahoo, or AOL, look closely at the link's address in the results before you click the link. Does it look normal? All reputable businesses will have a domain name that is easily recognizable. Some search results may show information that is pertinent to your request but will actually be malware cleverly disguised.

   Beware of domains that have nonsense names like strings of random letters and numbers. Also, be alert to where the domain is located in a web address such as in this fictitious example: www.yahoo.click52.com

   The domain name immediately before .com, .org, .net, etc. is the most important. In this instance, click52 (a fake, malicious domain) is using the word yahoo in their address to trick users. Note that the real Yahoo site could have a listing such as www.click.yahoo.com that is legitimate.

3. Because many children don't have the real world experience to determine unsafe situations or don't have well developed time management skills, **parental control programs** were created to help parents and guardians monitor computer activity. Most parental control programs will allow you to determine which sites are appropriate to visit, monitor time online, remotely manage computers, and restrict downloads - all excellent features to help protect sensitive information.

   If you have Microsoft Windows 7, you can download the free **Windows Live Family Safety 2011** through Microsoft's site (requires Windows Live account): http://explore.live.com/home

   Give us a call for more free and paid options.

4. If you are logging into a site through Wi-Fi, make sure that the address is using encryption like WPA. If you don't encrypt the data that you receive and send over a Wi-Fi connection, you risk having someone steal your personal information (neighbors included). When browsing in public Wi-Fi hotspots, always look for a secure connection to log into. Notice the additional 's' at the end of **https:** in the address bar not just http: or use a Virtual Private Network (VPN) for connecting.

5. Download **Malwarebytes**, an effective program to detect, log and remove malware.

   http://www.malwarebytes.org

   After you download this program, be sure to install updates to the software on a regular basis. The free version requires you to update the software manually while the paid version will download updates automatically. By downloading updates on a regular basis, you will ensure that you have the latest definition files to catch the most potential intrusions.

6. Sometimes pop-up screens appear unexpectedly on monitors. The box states that your computer has been infected and that you need to download software to clean your PC. If you click OK, malware is installed. Instead of clicking OK, click the X in the upper right corner of the box - you may need to click the X several times to close it. Again, DO NOT click the OK button. Then open Malwarebytes and scan your system immediately to make sure malware was not downloaded.