Q1 2013

INFORMATION PROTECTION NEWSLETTER

SHIELD

Secure Handle Involve Eliminate Learn Defend

Defending Your Home Computer Network

The Microsoft Safety and Security Center and OPPD Information Protection offer these seven tips to keep your home computer network safe from cybercriminals.

First, understand that you are a target, whether at work or at home

Cybercriminals use malicious software and deception to gain money from your bank accounts, your credit cards, and even your identity. Windows, Macintosh, and Linux home systems are now targets of their attacks. Their plans depend on your friendly, trusting nature and a lack of knowledge about how to recognize their attacks and keep computer equipment software and equipment secure.

Second, keep all software up to date

Cybercriminals tirelessly work to exploit vulnerabilities in software. Many software companies work constantly to combat these threats by patching these flaws when they are discovered. You can reduce the danger by updating your software whenever necessary.

Regularly install updates for *all* your software—antivirus and antispyware programs, Internet browsers (like Windows Internet Explorer, Safari, Firefox, Chrome), operating systems (like Windows, Mac OS, Linux), and word processing and other programs.

Ensure that you have the latest versions of third party Internet browser plug-ins, like Adobe Reader, Adobe Flash Player, Apple QuickTime, RealPlayer and others. These programs are often targeted by virus writers because they have weaknesses that can cause malicious software to be installed without your knowledge and users don't usually update them.

Subscribe to automatic updates whenever they are offered. To automatically update all Microsoft software, go to **update.microsoft.com**. Third party software providers offer similar update services.

Uninstall software that you don't use. This reduces the number of vulnerable programs cybercriminals can exploit. For Windows, you can remove it using Windows Control Panel.

Third, protect accounts with strong passwords

Strong passwords are long phrases or sentences that can mix or substitute letters, numbers, and symbols.

Keep passwords secret. Don't share them with anyone.

Don't use the same password on multiple sites. This is a common issue with social media sites and online shopping sites. Cybercriminals know this and will use your user ID (usually your email address) and password to get what they want – your money.

Create different strong passwords for the router and wireless key of your wireless connection at home. Find out how from the company that provides your router.

Fourth, never turn off your computer's personal firewall

A firewall puts a protective barrier between your PC and the Internet. Turning it off for even a minute increases the risk of a successful attack.

Your computer has a personal, software-based firewall that keeps attackers from gaining access to your PC without your knowledge. If you turn it off to troubleshoot a problem, don't forget to turn it back on.

If you use a small office home office firewall appliance between your service provider's equipment and your home network, ensure that its firmware is updated and it is not using a default password.

Fifth, use flash drives cautiously and minimize the chance that you'll infect your computer

Don't put *any* unknown flash (or thumb) drive into your PC.

To block malware, hold down the Shift key when you insert the flash drive into your computer. If you forget to do this, click in the upper-right corner to close any flash drive-related pop-up windows.

Don't open files from your flash drive that you're not expecting.

(Continued on page 3.)

Always use hard-to-guess passwords

$e7enal1ig@t0r5inmyb^th

(seven alligators in my bath)

Defending Your Home Computer Network (continued from page 1)

Sixth, don't be tricked into downloading malware

Be very cautious about opening attachments or clicking links in email or IM, or on social networks—even if you know the sender.

Because it has you're friend's address doesn't mean it's from your friend. Email accounts from popular webmail services are often hacked and the address books used to send malicious messages and spam to unsuspecting recipients.

Confirm with your friend that the message is OK. If not, delete the message or close the IM window.

Avoid clicking **Agree**, **OK**, or **I accept** in banner ads, in unexpected pop-up windows or warnings, on websites that may not seem legitimate, or in offers to remove spyware or viruses.

Instead, press Ctrl + F4 on your keyboard to close the window.

If that doesn't close the window, press Alt + F4 on your keyboard to close the browser. If asked, close all tabs and don't save any tabs for the next time the browser starts.

Seventh, install antivirus and antispyware programs from a trusted source

These programs scan and monitor your computer for known viruses and spyware. When they find something, they notify you and help you take action.

Never download anything in response to a warning from a program you didn't install or don't recognize that claims to protect your computer or offers to remove viruses. It's highly likely to do the opposite. In fact, it depends on you to help it get installed on your PC.

Get reputable malware protection from a vendor you trust. If your PC came with an anti-virus product, consider renewing the subscription when it comes due. Or choose from a list of Microsoft partners who provide anti-malware software often for Windows, Macs, and Linux PCs at **microsoft.com/windows/antivirus-partners**.

Otherwise there are free alternatives for Windows, Mac OS, and Linux. For example, Microsoft Security Essentials offers free real-time protection against malware. Sophos provides a free Mac OS AV product called Sophos for the Mac, and the open source ClamAV can be used for Linux PCs.

North American Electric Reliability Corporation (NERC)

Quarterly Update

Author: Mike Nickels

CIP-006 Requirement R1.6:

The NERC reliability standard CIP-006 requires that Visitors must be logged in AND out of individual NERC secure are-as. To accommodate this standard and provide proof OPPD is compliant to the standard, Corporate Security has placed a clip-board and signature sheet within each secure area (designated by previously installed red signs). Signatures are required from both the Visitor and the person escorting the Visitor.

A "Visitor" is **any** person that does not have permission to physically access individual NERC secure areas on OPPD property. To validate NERC CIP access, please look for the red stripe on the OPPD badge. Date and time must be entered when a Visitor both enters and exits a secure area. Corporate Security has placed the aforementioned clipboards and signature sheets in a visible location within each secure area. The following procedure is provided on the clipboards and is to be used when logging Visitors into and out of NERC secure areas:

- When a Visitor accesses a NERC secure area (designated by a red sign), the Visitor shall sign their name and provide location of employment, date, and time of access.
- The escort who allowed access to the Visitor shall also sign the log sheet.
- When the Visitor leaves the secure area, the escort at that time shall sign the log sheet and provide the time of exit for the Visitor.
- Visitors must be continuously escorted at all times while inside a NERC secure area.

If you have any questions regarding this process, please contact Rod Rogers, Manager – Corporate Security, at 636-3703 or Doug Peterchuck, Manager – Transmission Services, at 552-5181. Thank you for your cooperation.

February 2013 NERC Newsletter:

http://www.nerc.com/fileUploads/File/newsletters/NERCNews-2013-02.pdf

January/ February 3013 MRO Reliability Matters Newsletter:

http://www.midwestreliability.org/06_news/newsletters/2013/Newsletter_Feb_2013_Digital.pdf

Access Forms and CIP Cyber Security Policy:

http://insideoppd/Company/cip/Pages/default.aspx

THINK BEFORE YOU CLICK!

Information Protection would like to remind you to open each and every e-mail carefully. If you do not recognize the sender, do not open any attachments or click on links to websites. Doing so may result in your information being stolen (logins, passwords, etc.) and OPPD information becoming compromised. While we have scanning in place to catch (filter) some of these harmful e-mails, we cannot catch them all.

Some recent examples of malicious e-mails that reached OPPD users appeared to be e-mails can be viewed below. While these e-mails look legitimate, clicking on the links can both infect your computer and harvest information.

THINK BEFORE YOU CLICK. If you aren't expecting an e-mail from an institution or individual, have a questioning attitude. Do not click links or pictures within any questionable e-mail. If you receive a questionable e-mail, delete it. If you are unsure and feel that additional investigation is warranted, please contact Information Protection at informationprotection@oppd.com.

From: Twitter [mailto:e-nvqtpax=krdr-my.rk-2ee93@postmaster.riberofamily.it]
Sent: Wednesday, June 06, 2012 9:16 AM
Subject: Confirm your Twitter account!

Hi, mawortman@oppd.com.

Please confirm your Twitter account by clicking this link:
https://tyvitter.com/account/confirm_email/mawortman/8EA9D-81EF6-647443

Once you confirm, you will have full access to Twitter and all future notifications will be sent to this email address.

Thanks,
Team

If you did not sign up for a Twitter account, click not my account

FedEx

Order: RM-8723-2307345234
Order Date: Monday, 19 November 2012, 09:32 AM

Dear Customer,

Your parcel has arrived at the post office at November 29.Our postrider was unable to deliver the parcel to you.

To receive a parcel, please, go to the nearest our office and show this postal receipt.

GET POSTAL RECEIPT

Best Regards, The FedEx Team.

Subject: Order confirmation

You've just ordered pizza from our site

Pizza Ultimate Cheese Lover's with extras:- Pepperoni- Ham- Pepperoni- Black Olives- Black Olives- No Cheese- No SaucePizza Italian Trio with extras:- Italian Sausage- Ham- Jalapenos- Pineapple- Pineapple- Pineapple- Easy On Cheese- Extra SaucePizza Meat Lover's with extras:- Italian Sausage- Chicken- Pepperoni- Pineapple- Pineapple- Extra Cheese- Easy On SaucePizza Pepperoni Lover's with extras:- Pork- Diced Tomatoes- Jalapenos- Easy On Cheese- No SaucePizza Supreme with extras:- Pepperoni- Black Olives- Jalapenos- Diced Tomatoes- No Cheese- Easy On SaucePizza Veggie Lover's with extras:- Beef- Beef- Onions- Extra Cheese- Easy On SauceDrinks- 7up x 6- Dr. Pepper x 4- Squirt x 6- Diet Pepsi x 4- Coca-Cola x 5- Mirinda x 5Total to pay:231.61$

If you haven't made the order and it's a fraud case, please follow the link and cancel the order.
CANCEL ORDER NOW!

If you don't do that shortly, the order will be confirmed and delivered to you.

With respect
Pizza by ERMETE

Subject: Med Center Support

Welcome to Health Center

Hello,

You have been successfully registered in our Ticketing System

Please, login and check status of your ticket, or report new ticket here

See all tickets | View profile

If you have any questions, or if you believe that you have received this in error please contact us.

Thank you for contacting us!

Subject: Ticket [#32001910]

Thank you for contacting us, your information arrived today.

Alright, here's the link to the site:

Proceed to Site

If we can help in any way, please do not hesitate to contact us.

Sincerely, Dahlia Mclean, Support Team manager.