your energy partner®
OPPD
Omaha Public Power District

SHIELD
Information Protection Newsletter

SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND

When Free Software isn't Free

What is "Freeware"?

Many of us use freeware on a daily basis and don't even realize it. Freeware is software that is available for use at no cost to the user, for example, think of Skype or Adobe Acrobat Reader. In today's age of technology we have access to more software than ever before. Here are some basic safety precautions to help you remain safe.

The trend of bundling in extra software packages into installers is here to stay, unfortunately. More often than not when installing new software of the 'freeware' variety you will come across some subtle and less than desirable software bundles included in your installation process and even the most tech-savvy individuals have been fooled before.

What should I look out for?

More often than not the actual freeware or software that we intend to install is perfectly fine – Generally, the issues arise from the source in which we get it from. Affiliate programs with other freeware providers bundle packages together so that when you install the software you intended on using, like a browser, extra add-ons are installed at the same time: These may have other purposes, namely to cause your PC to make money illegally for cyber criminals and steal user information.

While these pieces of software may appear to have good intentions on the surface we have found over the years that this is not the case. For example, a search bar utility is a great place to sneak in 'spyware', tracking your search history and other private or personal information about the user that acts as a beacon, transmitting data covertly from their own machine without their permission.

Your browser might also be "hijacked" allowing a malicious program to participate in a advertising "click fraud" scheme where online pay per click advertisers are duped into paying a cyber-criminal for false clicks on their ads by PCs whose owners have never seen their ads. It might even be used to "mine" digital currency, such as Bitcoins, for cyber-criminals.

The best defense is a good offense!

if possible, **always** download software from the creator or publisher and not a third party vendor. When you install the software, read every page carefully. It is the 'dull' and 'boring' parts that we mindlessly click through every day that is where they will slip in bloatware, malware, and other packaged software.

If you cannot find a version of your software that is not riddled with extra software packages, consider a widely developed and well known open source equivalent. Open source software is different from freeware in that the source code (what makes the program) is readily available, is not proprietary, and is not monetized.

I think I may be infected

Please let us know about each instance of suspicious software you think might be on your work PC. Don't assume that it has already been reported to us and do not assume that it is not malicious.

Your timely report will help us understand the nature and scope of the incident. If you fail to report suspicious software to the Service Desk, you delay OPPD's response, thus exposing other OPPD systems to the risk of compromise. In your report, please let us know where you acquired the software, what its intended purpose was, and what you suspect has changed as a result of installing it, or, if you clicked on a link or opened an attachment. Please provide which OPPD device you used, such as a desktop, laptop, mobile device, etc.

It is your duty and your responsibility as an OPPD employee, not only for our organizations safety but also for our customers. **You are critical to OPPD's cyber security!**

Use Email Safely

Email is the number one method cyber criminals use to attack their victims. Be suspicious of odd emails or emails that seem too good to be true.

your energy partner®
OPPD
Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

OPPD IT Service Desk

Protect Your Internet Browsing

Hackers continually attack Internet browsers for all operating systems. These attacks exploit flaws in popular plugins, allowing hackers to take control of your PC. Follow these security principles to keep your devices safe.

Ensure you are using the latest version of your Internet browser on all devices at home or at work. Internet browser developers are continually adding new features and security measures. In addition they are continually patching their work as hackers find new ways to exploit software weaknesses.

Where possible, avoid using plugins and browser extensions While this extra software can add functionality to your Internet browser, it also adds many new flaws that hackers routinely exploit. For instance, Adobe Reader, Adobe Shockwave and Adobe Flash Player are heavily attacked. If you must use a plugin, ensure that it can be updated automatically. Check the plugin web site regularly for security advisories and patching information.

Scan everything you download. Use your regularly updated anti-virus scanner to inspect every file or program your download before you open them.

Enable all browser security features for your Internet browser and search engines. It's a good idea to periodically check your Internet browser's security features. For instance, in Internet Explorer, ensure that Smartscreen Filter feature is turned on. For Google Search, in the Search Settings options, ensure that SafeSearch is turned on and locked.

If you have doubts about a site, you can use the Google SafeBrowsing URL. Just enter the URL http://www.google.com/safebrowsing/diagnostic?site=google.com to return a report about the web domain. Change the "site=" portion of the URL to check out a new domain name.

your energy partner
OPPD
Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

IT-ServiceDesk@oppd.com

North American Electric Reliability Corporation

Quarterly Update

CIP-004-6 R2.3

CIP-004-5.1 Table R3 – Cyber Security Training Program			
Part	Applicable System	Requirements	Measures
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Require completion of the training at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

Beginning on July 1, 2016 OPPD Employees and Contractors with authorized electronic and/ or authorized unescorted physical access to OPPDs HIGH Impact BES Cyber Systems shall be officially notified and required to partake in the annual re-certification of OPPD NERC CIP Security Training. The annually recertification period begins Friday July 1, 2016 and will conclude on Friday, September 30th, 2016. OPPD employees who are currently NERC CIP authorized shall receive a notification via email on July 1, 2016. OPPD contractors who are currently NERC CIP authorized are to contact their OPPD sponsor for information pertaining to the re-certification training.

If training is not completed prior to September 30th, 2016 physical access and/ or electronic access to OPPD NERC CIP facilities and associated Cyber Assets will be revoked.

For more information pertaining to OPPD's NERC CIP Training or the Annual re-certification period, please contact , Mike Nickels – (402) 552-5036; manickels@oppd.com or Suzanne Krajicek – (402) 552- 5165; skrajicek@oppd.com .

your energy partner®
OPPD
Omaha Public Power District