SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter
your energy partner®
OPPD
Omaha Public Power District

Beware holiday phishing Grinches

The holiday season brings a flurry of gift-related emails intended by merchants to encourage online shopping and help folks track all those packages they ordered for the holidays.

Bogus package tracking notifications

During the holiday season, cybercriminal gangs do seem to net more victims with the fake package tracking notice ploy. Masquerading as shipping email from DHL, FedEx, UPS, and the U.S. Postal Service (USPS), the notifications may either contain a link to a malicious web site or a malicious attachment designed to download malware to your PC.

When activated, the downloaded malware may attempt to steal user credentials, banking and credit card information or attempt to encrypt important documents and hold them for ransom. Some of these phishing attacks may even try to coax you into supplying your address or banking information.

Expect these messages to look very official. If you are expecting a package from one of these vendors, you might be inclined to click on the link or open the attachment. Instead, take a moment or two to think through things before you click on something that could really ruin your holiday season.

In the case of bogus DHL shipping notices, the faked email contains the DHL color scheme and appears to be legitimate. Clicking on the embedded link in the message takes the user to an official looking web page that requests your user id and password. If enter this information, the attacker will harvest the email credentials and then access your mailbox.

A recent Fedex phishing attack uses messages claiming that a package sent to an unnamed recipient has been returned because of an incorrect address. The phishing messages urge the reader to open an attachment to view a shipping label or click on a link.

Beginning on December, 3, 2015 one phishing source sent out bogus package tracking emails from DHL, Fedex, and UPS and the U. S. Postal Service (USPS). These phishing email messages all contain a variety of attachments purportedly with package tracking information but actually containing malware. In a warning found at the FedEx web site, FedEx states that it does not send unsolicited email concerning packages, invoices, account numbers or personal information.

Fraudulent online payment notifications

In addition to fake shipping notifications, cybercriminals try to steal logon credentials for popular methods of making online payments, such as credit cards, online banks, and PayPal. Although the messages may look authentic, a closer look will reveal bogus email addresses and URLs that don't point to the correct company domain.

Attachments found in these messages also contain malware. These attacks may take the form of past due account warnings and expired password notifications.

Don't panic

Phishing email often contains alarming messages. These are intended to get you to click on a link or open an attachment. Take a deep breath and think through the message. If you think the message is valid, contact the shipping or online payment vendor through an 800 number posted at the vendor's web site. For credit or debit cards, call the 800 number on the back of the card to see if there is an issue with your card.

Remember your security awareness training to identify and report phishing messages to the IT Service Desk. Your You are an important part of OPPD's Cyber defenses.

Wi-Fi Security

Always use encryption when connected over public Wi-Fi networks.

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

At home or at work

Safely working remotely

With today's explosion of Internet devices and connectivity you can work from almost anywhere in the world. But with that convenience come new security threats through the very devices that make working from home so easy.

If you have been authorized to work from home remember that home networks and Internet connections are not as secure as OPPD's internal network. Connection to OPPD's internal network may be automatically denied if a potential security issue is detected.

Home networking equipment must be properly configured with firmware properly patched. Keeping these home networks updated is the responsibility of the employee or contractor.

Using a home Wi-Fi connection is allowed provided the wireless router is configured for Wi-Fi Protected Access 2 (WPA2). Use of a wireless mouse does not pose any significant security problems. However, wireless keyboards might be prone to interception, allowing a nearby attacker to capture what is being typed.

Issues regarding access speed may be caused by the Internet Service Provider or the number of devices accessing the home Internet connection. Employees and contractors should be able to work on documents and email even when Internet connectivity slows down.

Teleworking from public Internet connections should be avoided, since any Internet traffic through these connections is prone to interception. Places of heightened risk include airports, coffee shops and hotels.

Certain technologies and popular communications applications may not be allowed for teleworking because of security reasons. These include using peer to peer file sharing services and peer to peer chat services. These may be prone to compromise and cannot be guaranteed as being secure.

Please contact your supervisor and the IT Service Desk for any questions about working from home.

Working Remotely

If you have authorization to work from home or on the road, make sure you use only approved, secured devices.

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

North American Electric Reliability Corporation (NERC)

Quarterly Update:

NERC Cyber Infrastructure Protection (CIP) Version 5 Standards are here!!!

As 2015 comes to a close, the number of cyber-attacks are at an all-time high. One can only imagine what 2016 will bring. At OPPD, we will be migrating into the world of NERC CIP Version 5 which, in essence, will improve security efforts and increase compliance obligations. CIP Version 5 implements 10 standards and almost doubles the requirements and sub-requirement once held by CIP Version 3. A few of the more important changes within CIP Version 5 are as follows:

- **Encryption**
- **Role-based instead of risk-based classifications**
- **Multiple levels of compliance – Low, Medium and High Impact**
- **New terminology (such as BES Cyber Asset)**
- **All serial connections are to be considered**
- **Multi-factor authentication requirements**
- **Triggers are required to be defined for recovery plans**
- **All security patches from the beginning of time on each device must be known**

If you're an OPPD employee or an OPPD Contractor whose job requirements are NERC CIP related, the Reliability Compliance Department strongly recommends you get better understanding of the CIP Version 5 standards and requirements. OPPD employees, please feel free to contact OPPD's Reliability Compliance Department representatives for more information on CIP Version 5. OPPD contractors, please reach out to your OPPD Sponsors for CIP Version 5 information.

For more information pertaining to NERC CIP Version 5, please contact Doug Peterchuck, Manager of Reliability Compliance and Transmission Operations, dpeterchuck@oppd.com or Mike Nickels, Reliability Compliance Specialist, manickels@oppd.com

References:

NERC CIP Version 5: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

NERC CIP Version 5 Introduction: http://www.powermag.com/introduction-to-nerc-cip-version-5/