your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Three Unwise Holiday Cyber Ploys

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. Here are three cyber ploys it would be wise to avoid.

Bogus package tracking ploy

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.

Fraudulent online invoice ploy

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 fake online shopping invoice 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 that will be used to rob you. These attacks may take the form of past due account warnings and expired password notifications.

Deals too good to be true ploy

Last year, we ran a successful security awareness phishing test last year offering a bogus holiday shopping deal, so we know people may tempted to click.

Watch out for unexpected deals or promotions from vendors with whom do don't do business. The attackers are trying to fool you into ordering something you'll never receive or they are trying to "confirm" your payment credentials in order to steal them.

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.

Remember the slogan, "When in doubt, find out!' 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 Business Technology Service Desk. You are an important part of OPPD's Cyber defenses.

PII

Use only authorized systems to store, process or transfer Personally Identifiable Information (PII). Also, only share PII with authorized personnel who have a need to know.

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:
The Business Technology Service Desk
BT_ServiceDesk@oppd.com

Protecting the Internet of Things

This past year, hackers launched a highly successful series of very large distributed denial of service (DDoS) attacks that crippled parts of the Internet. Malware known as “Mirai” compromised large numbers of Internet-capable devices and turned them in a zombie army capable of compromising other devices and attacking Internet resources. The name “Murai” is the Japanese word for “the future,” and shows the intent of hackers to exploit Internet-capable devices.

This zombie army, or botnet, launched attacks against vulnerable Internet services without which the Internet comes to a grinding halt. In researching the attacks, investigators learned he compromised devices were home routers, networked DVRs, and Internet-capable security cameras. In short, devices that might be on your Christmas or tax-refund list.

Devices that can be controlled across the Internet are part of what is now called the Internet of Things (IoT) The IoT includes Internet-capable security cameras, home routers, entertainment systems, printers, thermostats, refrigerators, and even parking meters.

Here are three ways to protect IoT devices.

Check your IoT vendor’s site. Subscribe to your vendor’s email alert list. Periodically check for and apply any firmware updates. Check user forums for any security issues.

Disable any unnecessary ports and services. Your ioT device’s setup program should introduce you to the way to manage your device. Ensure that any Internet-facing management ports are turned off along with any unnecessary services.

Change default user names and passwords. Hackers know the default credentials and continually attempt to compromise IoT devices. Device setup should give you the ability to change the default login credentials. Then don’t delay, change credentials right away.

If you believe an OPPD IoT device has been compromised, report the incident immediately to the Business Technology Service Desk at 3848. You are an important part of OPPD’s cyber defenses.

Omaha Public Power District

This poster is published by OPPD’s
Cyber Security & Information Protection Department.
For more information, please contact us at:
The Business Technology Service Desk
BT_ServiceDesk@oppd.com

North American Electric Reliability Corporation Quarterly Update

CIP-003-7 Security Management Controls – LOW BES Cyber Systems

On December 5th, 2016, the NERC Standards Drafting Team (SDT) received approval by industry of recent modification made to the NERC CIP-003 standards. CIP-003 outlines the policy level requirements for High and Medium BES Cyber Systems as well as Low BES Cyber Systems. OPPD has continuously monitored this situation and has anticipated the proposed changes. So what's in store for OPPD and other entities? What's the impact of CIP-003 Version 7? Here is a few highlights of the changes made from Version 6 to Version 7.

CIP-003-7 addresses directives set forth by the Federal Energy Regulatory Commission (FERC). FERC requested modifications and additional "clarity" for Low BES Cyber System Electronic access controls. The CIP-003-6 R1.2.3 Electronic access controls for Low BES Cyber Systems included an assessment of Low Impact External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Points (LEAP). The assessment of LERC and LEAP left many entities searching for answers from their regional entities and NERC. To simplify this process, the SDT proposed the removal of LEAP and modified the definition of LERC. In changing the definitions of LERC, the SDT also modified the standard requirements for Electronic Access Controls. The new CIP-003-7 requirements for electronic access controls require only necessary inbound and outbound electronic access as determined by the Responsible entity for any communications that are:

- between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
- using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and,
- not used for time-sensitive protection or control functions between intelligent electronic devices

So what does this mean to OPPD and other entities who are in the process of implementing their Low BES Cyber system programs? Entities are encouraged to fully assess their Low BES Cyber systems within the current applicable standards approved by FERC. However, the realization that change is on the horizon must be accounted for. The effective date of CIP-003-7 will be the first day of the first calendar quarter that is eighteen (18) calendar months after the effective date of the applicable governmental authority's order approving the standard. OPPD's Reliability Compliance Department will continue to monitor the progress of CIP-003-7 as well as other NERC CIP Standards which are currently being modified by the NERC SDT.

For more information pertaining to compliance requirements for Low BES Cyber Systems or NERC CIP-003-7, please contact Reliability Compliance Specialist, Mike Nickels at (402) 552-5036; manickels@oppd.com.

your energy partner®
OPPD
Omaha Public Power District