your energy partner®
OPPD
Omaha Public Power District

SHIELD
Information Protection Newsletter

SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND

31 Days of Security Awareness Tips

Day 1 -- Avoid becoming a phishing victim by calling friends or colleagues who seem to be the senders of suspicious emails**.** Do not reply to the message until you verify its authenticity.

Day 2 -- Ask your tech-savvy children to teach you about using computers to help you learn what they are doing online**.** This will help you learn how to best protect them while they are online.

Day 3 – Encrypt sensitive data when it is stored on a mobile device or mobile storage device. If you believe the information you are authorized to store on a mobile device or mobile storage device requires extra security, contact the Service Desk.

Day 4 -- Set your home computer to receive automatic operating system and application updates since they contain security patches. Follow the same updating strategy with your mobile devices to keep them safe.

Day 5 -- Do not give out information about fellow employees, remote network access, organizational practices, or strategies to people you do not know**.** Verify the requester's identity before sharing sensitive information.

Day 6 -- When someone calls asking for private information, do not give it to them**.** Instead ask them for contact information so you can call them back at their place of work.

Day 7 -- Kids need extra protection online. Use a kid-friendly browser to ensure their safety. It is important to control the content that your kids can view online.

Day 8 -- You should only have access to the information you need to do your job. Report any irregularities to the Service Desk.

Day 9 -- Ensure that your data is protected at home. Encrypt hard drives and password protect devices. Use a password to protect all of your computers and devices and make sure that all the passwords you use are completely unique.

Day 10 -- Business cards aren't always real. Fake business cards may be used by criminals to gain access to certain areas. If you don't feel right about something, report it to the Service Desk.

Day 11 -- Identity thieves may use public forums to compromise someone's identity. Watch what you say about yourself or others. Remaining anonymous on the Internet is ideal.

Day 12 -- Your email password could be compromised if you use the same password elsewhere. Always use a unique password for each web site and change it often.

Day 13 – Your luggage can be lost or stolen. Never leave your luggage unattended and clearly label it with your name, address and phone number so it can be easily recovered.

Day 14 -- Bogus identity theft recovery services target identity theft victims. Don't get robbed twice. Hang up on these scammers.

Day 15 -- Your laptop is fragile. Many people use their laptop in bed. To avoid damage, place your laptop somewhere safe before falling asleep.

Day 16 -- Photos and text you send to others never go away and they can be copied by bad guys.

(Continued on page 2)

31 Days of Security Awareness Tips

(Continued from page 1.)

Day 17 -- Malware can be anywhere. Always use antivirus protection and set it to automatically update to help counter new security risks.

Day 18 -- Always be careful about your actions when working with confidential information. Immediately report the exposure of confidential data and loss of equipment containing confidential data.

Day 19 -- Always follow acceptable use policies for mobile devices and data to minimize loss of confidential information. Enable the "remote wipe" feature of your smartphone so you can delete files if your device is misplaced or stolen.

Day 20 -- Protect your data when on wi-fi by only using secured wireless access points and secure web sites that use HTTPS. When outside the company network, assume the wi-fi connection is not secure.

Day 21 -- Avoid donation scams by verifying the sender's identity. Make donations directly to the charity instead of relying on an intermediary party to make the donation on your behalf.

Day 22 – When traveling leave copies of your id and passport along with your complete itinerary with someone back home. This way, if you lose your ID, the person can send you a copy or alert the authorities if you go missing.

Day 23 -- Social media can be dangerous. Use strong privacy settings to reduce the risk. When in doubt, refrain from sharing too much personal information online.

Day 24 -- Scan your email messages with antivirus software. Enable your antivirus software's auto-protect feature to automatically scan email attachments for viruses. Ensure your antivirus software also detects viruses based on their behavior and not just AV updates.

Day 25 -- Secure your work area from physical security threats. Put away documents containing sensitive information when you leave your work area. Always lock your computer screen when you take breaks or leave for the day.

Day 26 -- Secure your data when browsing the web by using encrypted sites. To ensure safer web browsing, make sure that every site that you give information to uses encryption. Make sure web sites have a valid security certificate and that they are using "https" rather than "http."

Day 27 -- Protect your data by identifying sensitive information, restricting its access, and encrypting it**.** Store sensitive data in an encrypted format, especially when using mobile devices and mobile storage media.

Day 28 -- Hover your mouse cursor over URLs in emails to make sure they're legitimate.
The display name of the website might be for a company that you already trust and use, but the actual link takes you to a fake or copycat website designed to steal your account's login information. When in doubt, don't click.

Day 29 -- "Tailgating" is a common method used to gain access to restricted areas. Don't let others in when you use your badge. You should never let another person follow you into a restricted area. Their credentials may have been revoked and you may not know.

Day 30 -- Scam artists may use your social media to make their emails more convincing. Remain skeptical about any unsolicited emails. Avoid helping scam artists by keeping as much of your personal information off of social media as possible.

Day 31 -- Never ignore cyber bullying. Even anonymous cyber bullies can be traced by the authorities. Document every instance of bullying and bring it to the attention of your school and the local authorities so that they can identify the bully.

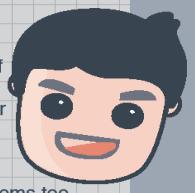
How to Spot a Phish

Finding the phish 101 with Professor Troy

Lesson 1: Watch out for emotions

Greed

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems too good to be true, it probably is.



Urgency

If an email provides a strict deadline for performing an action -- be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.

Curiosity

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.

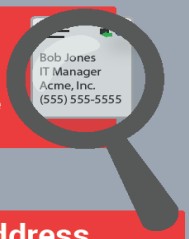
Fear

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

Lesson 2: Examine these items closely

Email Signatures

A signature block that is overly generic or doesn't follow company protocols could indicate that something is wrong.

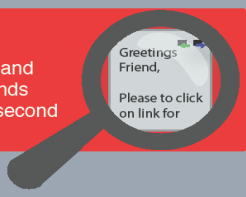


Sender Address

If the address doesn't match the sender name, be suspicious of the entire email.

Email Tone

We know how our co-workers and friends talk, so if an email sounds strange, it's probably worth a second look.



Lesson 3: Beware of these elements

From: Joe Smith
To: Troy Foster
Subject: WebMail Migration

Attachment -- Webmail_Migration.pdf

Attachments

When an attachment comes from someone you don't know or if you weren't expecting the file, make sure it's legitimate before opening it.

Troy,

This is to inform you that we are in the processing of m
to the Windows 2003 platform, which includes an exci
e-mail.

Log-in Pages

Spear phishers will often forge login pages to look exactly like the real thing in order to steal your credentials.

Attached is a document outlining the benefits of the m
migration we request you to enter your Windows password before 8 PM on Tuesday.
Failure to do so will result in being locked out of your email account!

Please click here to update your password.

Thank You,
John Smith

Links

Roll your mouse pointer over the link and see if what pops up matches what's in the email. If they don't match, don't click.

If you see something, say something!

Report suspected phishing emails to the information security team

PHISHME

North American Electric Reliability Corporation Quarterly Update

CIP-010-2 Requirement 4: Transient Cyber Assets and Removable Media

On April 1st, 2017 OPPD will be expanding the NERC CIP Program into an area that has been somewhat controversial over the years. If you've followed the cyber-security landscape over the last few years, you've noticed an increase of hacking and system infiltrations into corporations, utilities and other organizations which upon completion of forensics it was found that the initial hack consisted of a universal serial bus (USB) device being plugged into a critical network and malicious code being executed. The Federal Energy Regulatory Commission (FERC) realized the risk and the common vulnerabilities associated and ordered NERC to establish security standards to minimize the risk to the Bulk Electric System (BES). Enter in CIP-010-2 R4:

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media.

The plans within the standard addresses oversight and governance of Transient Cyber Assets (Laptops, testing equipment, etc.) and Removable Media (USB, CD ROM, portable hard drives, etc.) by implementing the following:

- Transient Cyber Asset Management
- Transient Cyber Asset Authorization
- Software Vulnerability Mitigation
- Introduction of Malicious Code Mitigation
- Unauthorized Use Mitigation
- Removable Media Authorization
- Removable Media Malicious Code Mitigation

OPPD has been developing and planning the implementation of CIP-010-2 R4 for quite some time. OPPD's Subject Matter Experts (SME) have developed and implemented their plans to address the CIP-010-2 R4 standards. For those individuals whom work within or around OPPD BES Cyber systems, please ensure to discuss this new requirement with your BES Cyber System Owner and understand the role and responsibilities within your set program.

For more information pertaining to CIP-010-2, Transient Cyber Assets and Removable Media, please contact Reliability Compliance Specialist, Mike Nickels at (402) 552-5036; manickels@oppd.com.

Resources:

NERC (January 2016) CIP-010-2 Cyber Security – Configuration Change Management and Vulnerability Assessments. Retrieved from: **http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-010-2&title=Cyber Security - Configuration Change Management and Vulnerability Assessments&jurisdiction=null**

your energy partner®
OPPD
Omaha Public Power District