your energy partner®
OPPD
Omaha Public Power District

SHIELD
Information Protection Newsletter

SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND

Five things to combat Phishing

Phishing is a cyber-security term for the use of specially-crafted email to deceive the reader into revealing financial or other confidential information. The email often mimics content from a legitimate entity, like a financial company or even a personal friend. The email could be complex, html-based email or a simple text-based message.

Through the email's content, the reader is enticed to open an attachment or click on a link in the message. Once you access the malicious content, your PC can be compromised or you may be enticed into providing valuable information, such as account numbers and login credentials.

To help you defend yourself and OPPD from these cyber attackers, here are five things you should do to fight phishing attacks.

First, educate yourself about phishing. Learn to recognize the elements of a phishing attack. OPPD's security awareness web pages found in the left hand column of the Inside OPPD home page, contains many excellent short cyber security videos that arm you with the knowledge to help hold cyber attackers at bay. Each video comes with a short quiz to help gauge your understanding of the threat. We recommend you view "***Securing the Human: You Are the Target"***, "***Securing the Human: Email and Messaging Attacks"***, and "***Securing the Human: Social Engineering"***. If you are in a supervisory position or have access to sensitive information, please view "***Securing the Human: Advanced Persistent Threat (APT)"*** for a better understanding of how you are being actively targeted by cyber-criminals so the information you can access could be stolen or destroyed.

Second, read every email with a critical eye. Using the knowledge you gained through viewing OPPD's security awareness videos, think before you click a URL or open an email attachment. There is an old Portuguese proverb that states, "Haste is the enemy of perfection." Likewise, the enemy of cyber security is hasty decision-making. In interviews after a phishing incident, we often hear the victims say they had been in a hurry to get through their email and realized immediately afterwards that they had been tricked into acting on the phishing email's content.

Third, don't play detective. When you receive unexpected email, do not reply to the email to find out if the email is legitimate. When you reply to the phishing email you identify yourself as a living person. The attackers now know your email address is valid and they will launch follow-on attacks. Additionally, they will use information contained in your message and email signature to masquerade as you or provide more intelligence for attacks against OPPD.

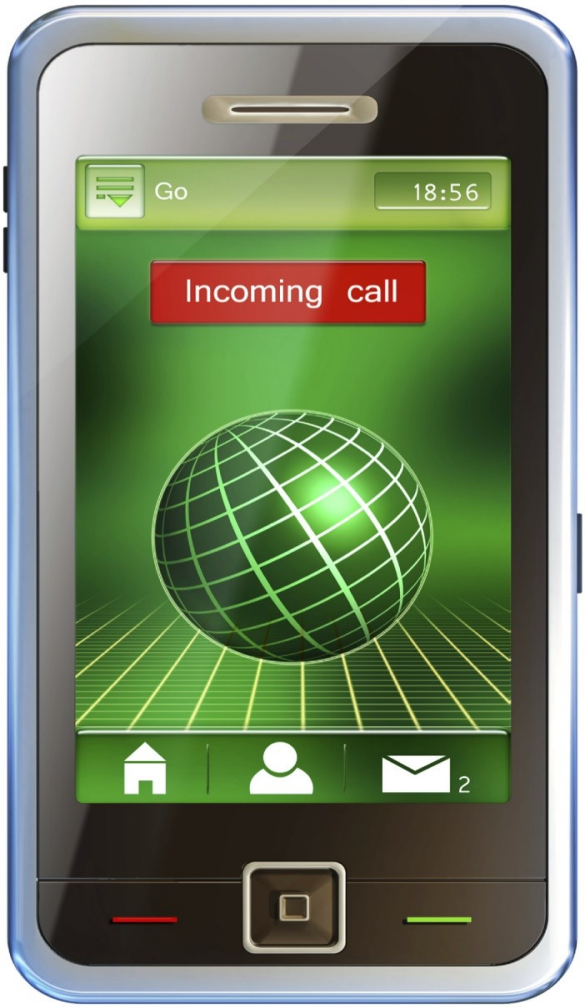
Fourth, report the phishing activity to the Service Desk. Please let us know about each instance of a suspicious email. Don't assume that it has already been reported to us. Your timely report will help us understand the nature and scope of the attack. If you fail to report phishing attacks to the Service Desk, you delay OPPD's response the new phishing attacks, thus exposing other OPPD systems to the risk of compromise. In your report, please let us know if you clicked on a link or opened an attachment and which OPPD device you used, such as a desktop, laptop, mobile device, etc. Many phishing attacks use malicious resources and malware initially unknown to cyber security vendors. Your report will help us remove a potentially compromised computer before it can do harm to you, OPPD and our customers. We can then analyze it for malware or signs of compromise that will help us combat other phishing attacks.

Fifth, share your anti-phishing knowledge with others. Talk to co-workers and family members about what you've learned through OPPD's security awareness videos, the ***SHIELD*** newsletter, or cyber security ON Story articles. If you are a supervisor, regularly discuss phishing incidents with your staff as part of your group's security awareness training efforts. Ensure that all employees know where to find the Security Awareness page and view the contents.

Please remember that you are a valuable part of OPPD's cyber security defenses. By using these five steps to combat phishing you will help keep OPPD and our customers safe from cyber-attack.

Mobile Devices

Lock your mobile devices with a PIN or password, always keep them updated and do not trust odd messages.



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

Four things to counter Social Engineering

Some people believe that all cyber-attacks are perpetrated by hackers using complicated programs and tools. This isn't true. However clichéd it may seem, the most vulnerable part of any system is its users and people can be exploited in a variety of ways.

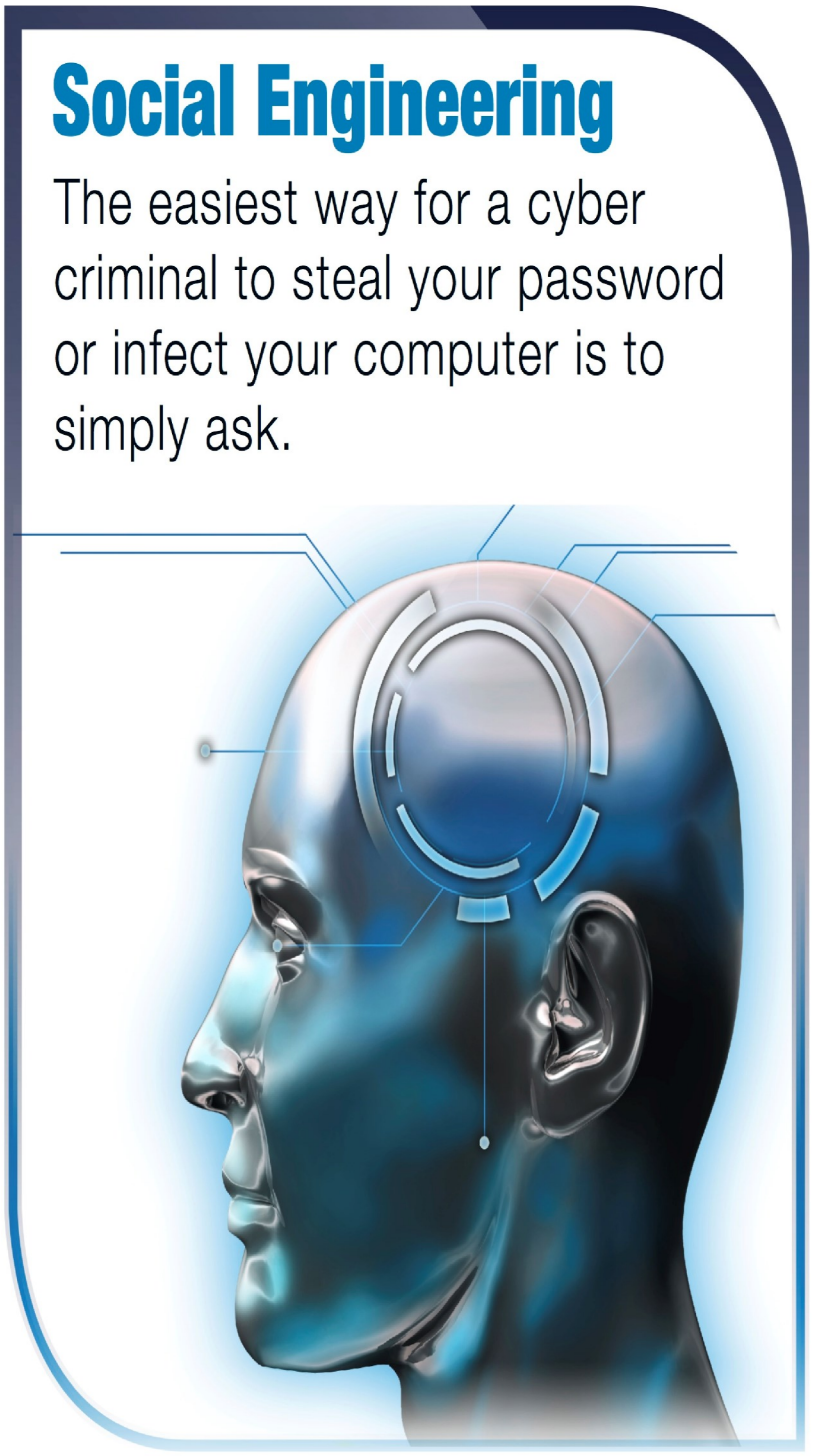
These methods are commonly referred to as "social engineering" or the art of human manipulation. Simply put, it is the art of tricking people into doing things they normally wouldn't, such as breaking cyber security procedures.

These techniques aren't new. There have been "con men" as long as there have been people. Technology has allowed these attackers to a reach much wider audience in a more efficient manner. It is becoming increasingly common that you will be subject to a social engineering attack, so understanding ways to identify these schemes is important.

Be sure to follow these tips:

- Be skeptical. If you feel apprehensive or strange, trust your instincts and leave the situation.
- Never give out any confidential information to anyone without verifying the identity of the person and their need for using it. Most companies will not ask you for that information over the phone.
- Be careful what you post on social media. Many scammers use public knowledge to their advantage to trick you into revealing more sensitive information. Even a seemingly innocent post can be mined for material.
- Social engineering is not done exclusively through any one medium. It can occur over the phone, through a text message, in an email or even in person!

Keeping these things in mind will not protect the company from unnecessary exposure but your personal network and data as well.



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

North American Electric Reliability Corporation

Quarterly Update

Physical Security Plan – CIP006-6 Requirement 1.3

As NERC approves the new revisions of the Cyber Infrastructure Protection (CIP) requirements, entities are planning and implementing their strategies not only to meet compliance obligations but to increase security measures. CIP006-6 Requirement 1.3 was developed by the NERC CIP Standards drafting team to provide a defense in depth approach by utilizing two or more different and complementary physical access controls. OPPD has implemented the "two-factor authentication" at specific locations and due to the new requirements, OPPD employees and contractors possessing or applying for physical NERC CIP access will require to have a OPPD NERC CIP Badge and a personalized five digit PIN to access these specific locations.

In addition to the two-factor authentication, OPPD still maintains standard security measures to ensure the reliability of our facilities. OPPD's Visitor Control Program establishes the process of controlling escorted and unescorted access into specific NERC CIP Areas. In addition to escorting and escorting responsibilities, the Visitor Control Program also addresses, Visitor Access Logging and On-site Security Screening Measures.

Finally, as stated within the OPPD Security Operating Policy, Tailgating – The unauthorized act of following another person (who is authorized to gain entry into a restricted or access control area) into a restricted or access controlled areas without utilizing their own access card, or being escorted by an authorized person- Shall not be permitted.

If you are an OPPD employee or OPPD contractor with authorized physical NERC CIP access please ensure you familiarize yourself with the security processes in place.

If you have any questions regarding NERC CIP requirements or OPPD NERC CIP compliance obligations please contact Mike Nickels, Ext. 5036, manickels@oppd.com.

References:

OPPD's Security Operating Policy

OPPD's NERC CIP Visitor Control Program

OPPD's NERC CIP Physical Security Plan

OPPD's NERC CIP Cyber Security Policy

your energy partner®
OPPD
Omaha Public Power District