your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND

Information Protection Newsletter

Phishing Emails are <u>NOT</u> the <u>ONLY</u> threat...

Social Networking sites - Friend OR Foe?

Perhaps you are a "reformed clicker" and have been made aware of the threat posed by attackers who Phish for trusting people who click on links and attachments in an email that is cleverly designed to look innocent. But what about Social Networking sites like FaceBook, Twitter, or LinkedIn. They are secure, right? WRONG! Not everyone on FB, Twitter, or LinkedIn is your friend!

Attackers can easily create a robot account to mimic a real person and can even capture YOUR INFORMATION and create a false account that looks just like you, or like one of your friends!

There are many horror stories regarding data breaches and potential breaches due to Social Networking scammers attacking unsuspecting victims.

One of the most famous is the 2009 creation of the fictional persona "Robin Sage" by Thomas Ryan, a controversial security specialist and "white hat" hacker from New York City. During the time her identity was active on popular social networks like Facebook, LinkedIn, Twitter, etc.; her identity was used to contact nearly 300 people, most of them security specialists, military personnel, staff at intelligence agencies and defense contractors. Despite her completely fake profile, and no other real-life information, Sage was offered consulting work with notable companies and received dinner invitations from several of her male friends. The findings of Ryan's short experiment were presented at the "Black Hat" conference in Las Vegas. He showed how using the contacts in her Social Networking sites, she gained access to email addresses, and bank accounts, as well as learning the location of secret military units based on soldiers' Facebook photos and connections between different people and organizations. She was also given private documents to review and was offered to speak at several conferences.

While not everyone was fooled by Sage's profiles, no central warning was issued about the profile, and users continued to connect with Sage despite warnings not to do so.

This short experiment also proved that seemingly harmless details shared via social networking pages can be harmful; but also that many people entrusted with vital and sensitive information would share this information readily with third parties, provided they captured their interest. He concluded that his findings could have compromised national security if a terrorist organization had employed similar tactics. [1]

Another recent article in the New York Times (May 28, 2017) warns Hackers Hide Cyberattacks in Social Media Posts!

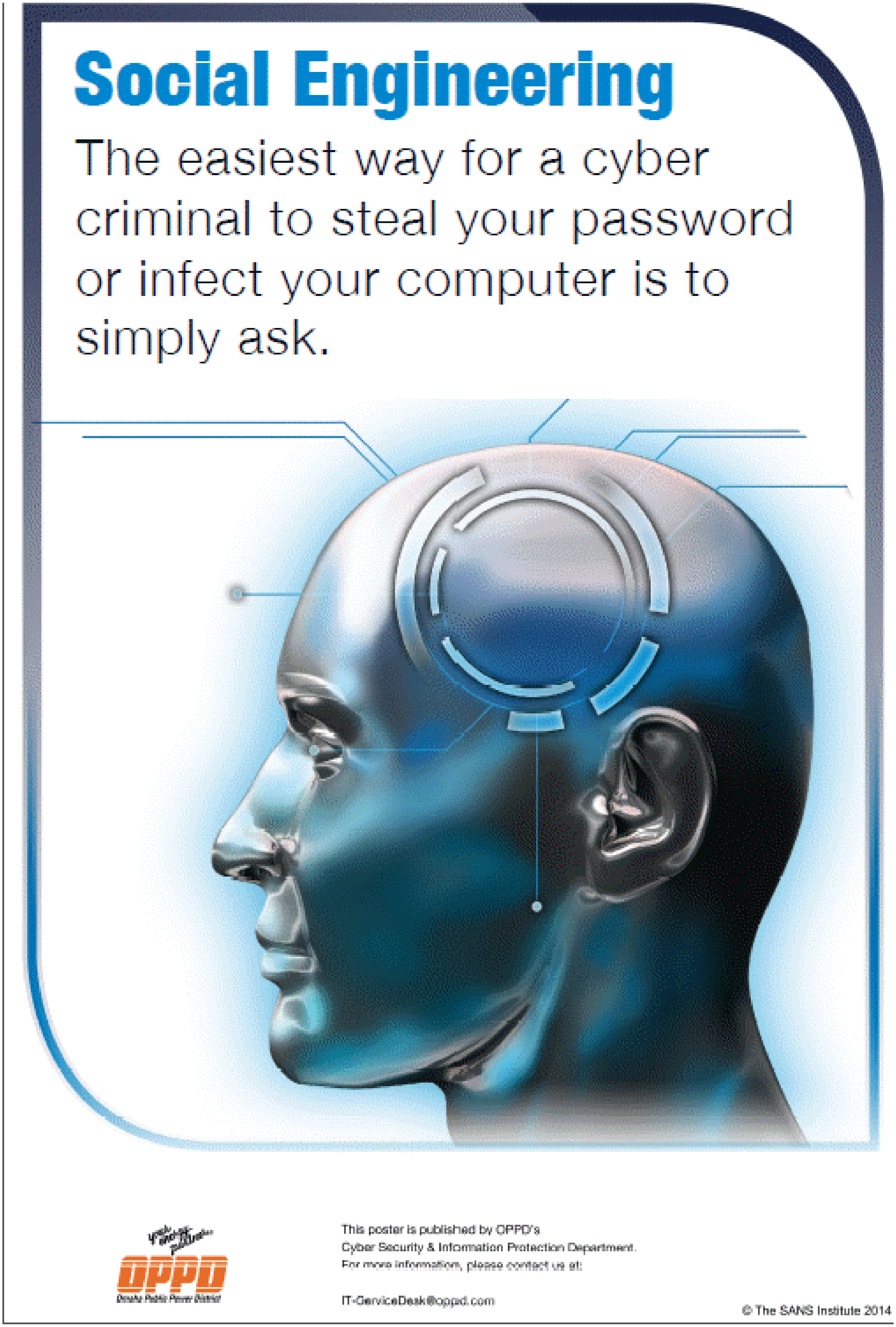
Even an apparently innocent link to a potential family vacation get-away spot in Twitter can have devastating consequences...IF it comes from a Hacker! While corporations and government agencies are training staff to think twice before opening anything sent by email, hackers have already moved on to a new kind of attack, targeting social media accounts, where people are more likely to be trusting. The human error that causes people to click on a link sent to them in an email is exponentially greater on social media sites because people are more likely to consider themselves "among friends".

Cybersecurity companies said spear phishing through social media was one of the fastest-growing methods of attack.

It's something that you don't hear as much about, but the problem is pervasive," said Jay Kaplan, a former Defense Department cybersecurity expert and senior cyber analyst at the National Security Agency who is now the chief executive of the cyber security company Synack. "Social media gives a number of indicators to an attacker, on a state-sponsored level, that you couldn't get through email."

According to a 2016 report by Verizon, roughly 30% of spear phishing emails are opened by their targets; while research, published by the cybersecurity firm ZeroFOX showed that 66% of spear phishing messages sent through social media sites were opened by their intended victims.

(Continued on pg. 3)



Social Engineering

The easiest way for a cyber criminal to steal your password or infect your computer is to simply ask.

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

(Continued from pg. 1)

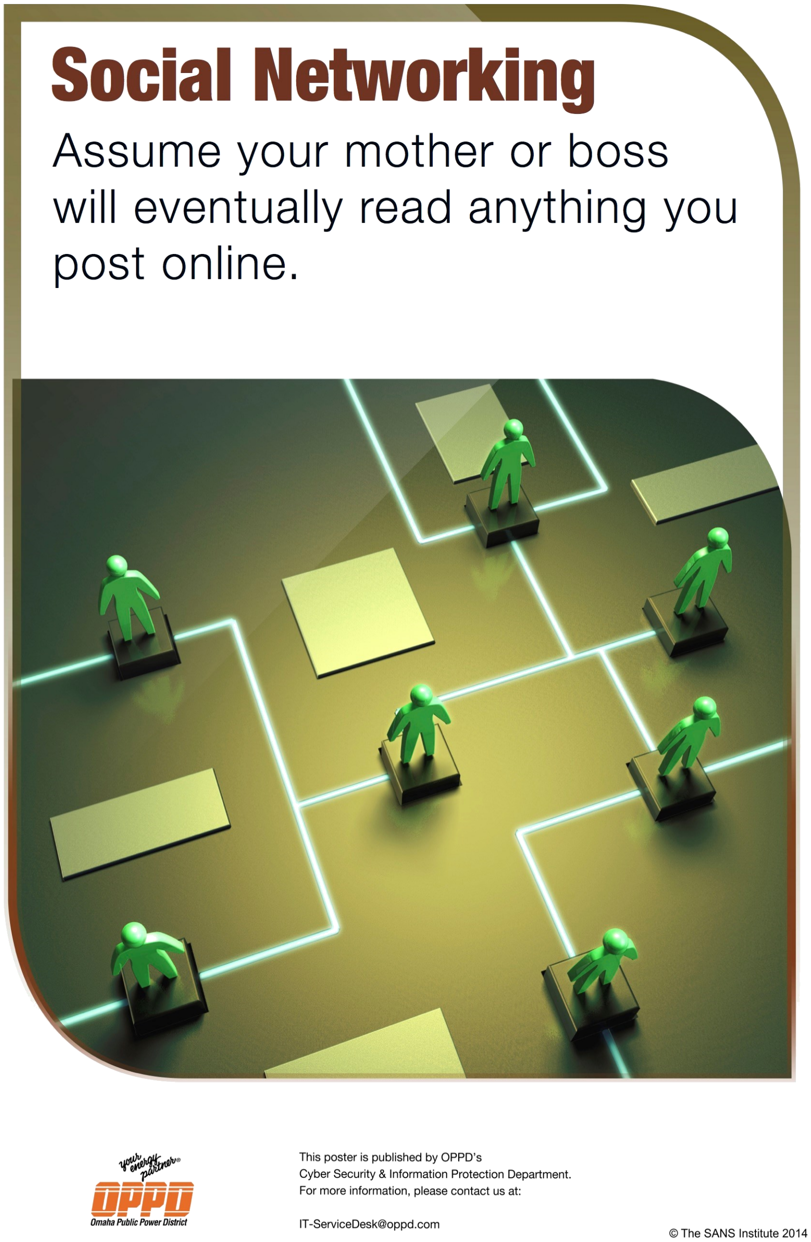
In the Defense Department attack, for example, 7,000 employees took the first step toward being compromised by clicking on a link, said Evan Blair, a co-founder of ZeroFOX. “The attacks are so much more successful because they use your personal timeline and the content you engaged with to target the message to you,” Mr. Blair said.

Mr. Blair also said that, in the case of the Defense Department, the links had carried the malware. Once people clicked on the link, they were infecting their computer networks. In many cases, the attackers targeted members of Defense Department employees’ families, who were less likely to be suspicious.

The Defense Department employee who told The Times that he had been part of the recent breach said he had been targeted through his wife’s Twitter account. She was the one to click on a link to a vacation package, after exchanging messages with friends over what they should do with their children over the summer. Once the hackers got into her computer, the official said, they got to his computer through a shared home network.

The moral to this story: *Be aware* of the threats that exist on Social Networking sites, and *take measures* to secure your identity through the Security features of the site, AND follow the **5 Things to Remember** below.

[1] https://en.wikipedia.org/wiki/Robin_Sage



Social Networking

Assume your mother or boss will eventually read anything you post online.

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

IT-ServiceDesk@oppd.com

© The SANS Institute 2014

5 THINGS TO REMEMBER about sharing information on **Social Networking** sites:

1. **Be careful what you share.** Details about your personal information can be used to steal your identity, guess passwords, or engage in fraudulent behaviors.
   - Privacy Controls are not always effective in protecting your information
   - Assume that **EVERYTHING** you post **WILL EVENTUALLY BECOME PUBLIC**.
2. **Be careful what your friends post** about you and **monitor** *their postings about you.*
   - If it is confidential or inappropriate, ask them to remove it or report it to the Social Media's abuse department.
3. Hackers can access accounts and post things while pretending to be YOU (OR your Friends); for instance posting fake messages asking for help/money, etc.
   - If suspicious messages come from a friend, call them to verify the authenticity of the message.
4. **Third Party applications that integrate with a Social networking sites** can also be infected or may attempt to access your personal information.
   - **ONLY install** applications that you **NEED, and ONLY** get them **from TRUSTED SOURCES**.
   - When you stop using any application, uninstall it and/or disable it's access to your social networking profile.
5. **DO NOT POST ANY CONFIDENTIAL INFORMATION ABOUT WORK on ANY WEBSITE.**

North American Electric Reliability Corporation Quarterly Update

CIP-004-6 Requirement 2 – Cyber Security Training Program

Each Responsible Entity shall implement one or more cyber security training program(s)
appropriate to individual roles, functions, or responsibilities.

In adhering to NERC CIP standard, CIP-004-6 R2, OPPD has implemented the OPPD NERC CIP Security Training Program, which requires all employees and contractors requesting NERC CIP access to OPPD's BES Cyber Assets and OPPD's BES Cyber Systems to complete detailed cyber security training prior to access authorization. In addition, OPPD employees and contractors who are currently authorized for NERC CIP Access are required to perform annual training every 15 calendar months. OPPD's NERC CIP Security Training Program has been designed to bring awareness, insight, and a constant reminder of the importance of OPPD's security standards involving physical and electronic security to those individuals who work in and around OPPD's BES Cyber Assets and BES Cyber Systems. OPPD's NERC CIP Security Training Program covers Cyber Security polices, Physical access controls, Electronic access controls, OPPD's Visitor Control Program, Information Protection methods, Cyber Security incident response, recovery of BES Cyber Systems, and overall risk associated with OPPD's BES Cyber Assets and BES Cyber Systems.

Beginning on July 1, 2017 OPPD Employees, OPPD Sponsors and contractors with authorized electronic and/ or authorized unescorted physical access to OPPD's HIGH Impact BES Cyber Systems shall be officially notified and required to participate in the annual re-certification through the OPPD NERC CIP Security Training. The annually recertification period begins Saturday July 1, 2017 and will conclude on Saturday, September 30th, 2017. OPPD employees who are currently NERC CIP authorized shall receive a notification via email on July 1, 2017. OPPD Employees shall complete the required training via OPPD's Training Partner application, located on the OPPD intranet home page under **Corporate Systems**. OPPD contractors who are currently NERC CIP authorized are to contact their OPPD sponsor for information pertaining to the re-certification training.

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 Shayla Mc Donnell – (402) 552-5165; smcdonnell@oppd.com.

your energy partner®
OPPD
Omaha Public Power District