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

Social Engineering isn't a prank

All of us can remember falling for an April Fool's Day prank where we were tricked in believing something only to find out when the pranksters shouted "April Fool's" that you were the butt of a practical joke. While April Fool's Day happens only once a year, unfortunately there is a form of cyber deception called "social engineering" that happens 24 hours a day, seven days a week.

Like the traditional April Fool's Day hoax where the prank is made by someone you know, social engineering attackers start by posing as someone you know or a trusted organization. They send their messages through media that you've come to trust such as phone calls, instant messages, or email on devices that you trust such as personal computers, tablets, and smart phones.

Since these technologies are worldwide in scope, it is easy for the attacker to be anywhere in the world. Since these communications methods have to be fairly simple, it is also very each for the attackers to disguise their true natures and geographical locations. Therefore the person you think might be in the same building or city may be an attacker on another continent.

Experts at SANS.org state it's important to remember that social engineering isn't a technical attack. It's a psychological one that plays on our natural impulse to be helpful to others. Cybercriminals know that rather than using technical means to break into computer systems, it's much easier just to ask the computer users for the information that they need to launch an attack.

Social engineering attacks are very difficult to stop since technology alone can't prevent someone from innocently telling sensitive information to a cybercriminal. The best defense is for everyone at OPPD to develop a questioning attitude and report a suspicious interaction to the OPPD IT Service Desk.

First, understand that you are a target. Whether you believe it or not, you have information or know someone who has information that could help cybercriminals conduct their attacks.

Secondly, the best way to protect yourself is to use common sense. If something about the message or phone call seems absurd or too good to be true, trust your instincts. It is likely a social engineering attack. Here some examples to consider.

- In one social engineering attack, hotel occupants received a phone call from someone claiming to work for the hotel The attacker stated she needed confirmation of the credit card billing information in order to correct a clerical error. It was only after the credit card numbers were abused that the owners realized that they had been tricked by someone who was half a world away rather than a hotel employee.
- Cyber criminals will also use official looking emails from banks or other organizations explaining that user accounts have been locked for security reasons. These messages urge the readers to click on links in the messages to confirm user accounts and passwords. In other variants of this attack, users may get messages stating that they have documents waiting for them onfile sharing sites and all they have to do to get them is to enter their email addresses and passwords.
- You may also encounter messages that play to greed, announcing that you've won a lottery, when in fact you never entered the lottery. In order to collect the winnings you are supposed to contact someone and supply your banking information. When you contact the person, they explain that you much first pay a fee to collect the prize. The real goal is to steal your money and there isn't any prize money.
- You may also get an email or a social media message from a friend visiting a foreign country who has run into difficulties and needs a loan in order to get home. The truth of the matter is your friend is not visiting a foreign country. Instead their email or social media account has been hacked. Use other means to contact your friend to confirm that they are not in trouble rather than believing the cry for help.
- Finally, you might get a phone call from someone claiming to belong to a technical support organization. This person will claim that your PC is infected and they need access to your PC in order to fix the problem. Their real goal is to gain control of your PC so they can plant Trojan horses and steal your sensitive personal information.

You Are The Target

Your accounts, computers and devices have tremendous value to cyber criminals. The first step to protecting yourself is understanding that you are under attack.

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:

OPPD IT Service Desk

Advanced Persistent Threat

They’re gunning for OPPD staff

As a utility, OPPD faces a more sinister cyber enemy than the garden-variety cybercriminal interested in stealing credit card numbers. This foe is called an Advanced Persistent Threat (APT).

This is not a single cybercriminal, but rather a team of skilled specialists whose mission is to study OPPD’s organization and devise ways to gather information for their own organization’s objectives.

Because we are in power generation business, APT teams are ultimately interested in disrupting our systems to cause blackouts or even long term damage. APT teams are not a theoretical threat. They are well known to national security agencies and come from current and potential adversaries.

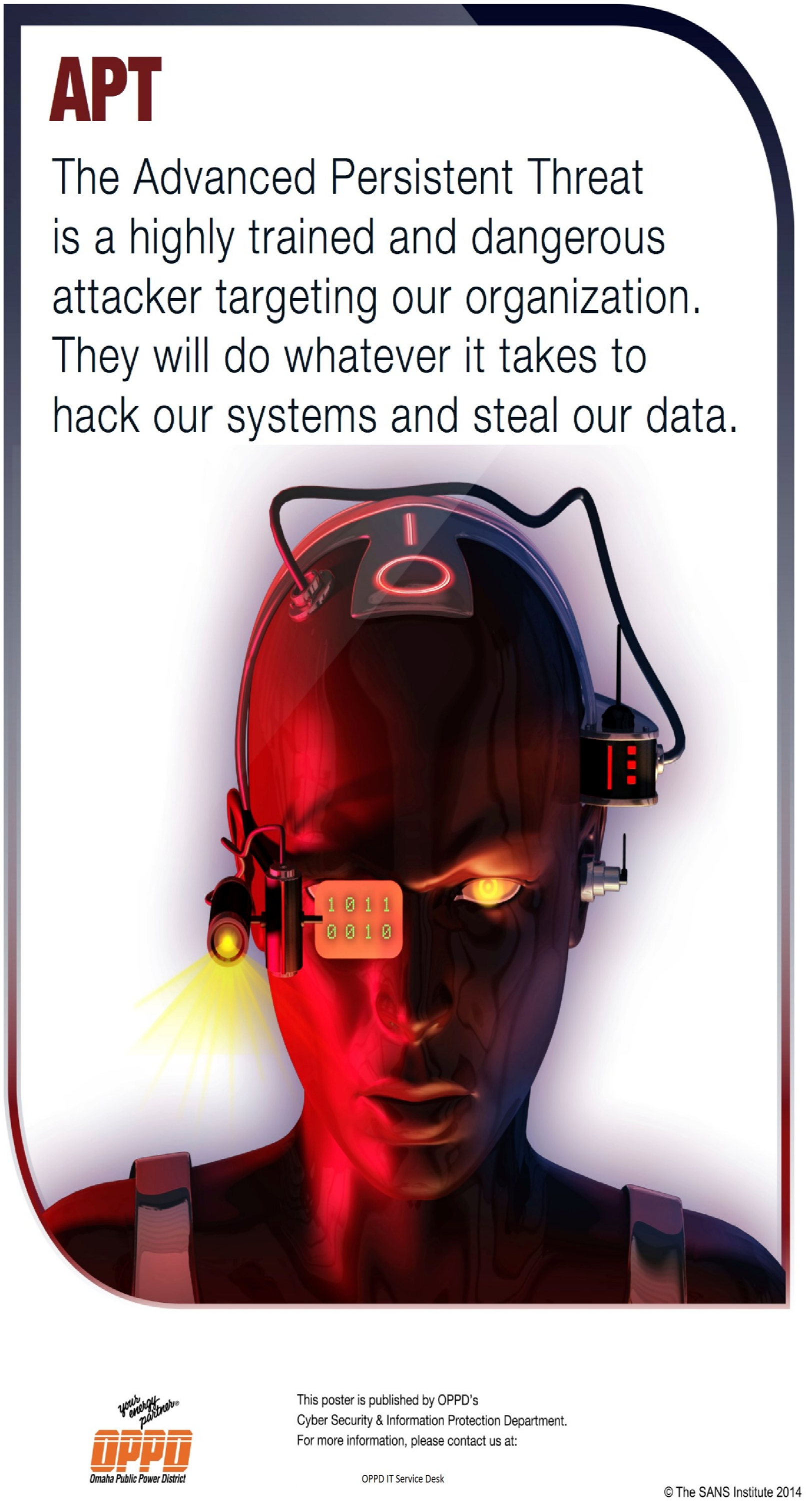
APT teams are assigned potential target organizations which they research in order to identify executives and staff members that have access to sensitive information. They then research these individuals in order to launch highly customized attacks against them.

Because they are selecting their targets from a smaller number of people, it can be difficult to spot an APT attack.

The best way to protect yourself and OPPD from APT attack is to limit the amount of information you post to the Internet. Using such data, an APT team can make social engineering attacks though phone calls and emails that are believable because of the amount of information the APT team knows about you.

According to SANS.org, APT attacks are some of the gravest cyber threats to OPPD and our nation.

You can help stop this wily enemy by reporting any odd phone calls, emails, or emails with strange attachments or links to the OPPD IT Service desk.



APT

The Advanced Persistent Threat
is a highly trained and dangerous
attacker targeting our organization.
They will do whatever it takes to
hack our systems and steal our data.

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:

OPPD IT Service Desk

North American Electric Reliability Corporation (NERC)

(Quarterly Update)

CIP-004 -3 R1- Security Awareness

Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

Direct communications (e.g., emails, memos, computer based training, etc.);

Indirect communications (e.g., posters, intranet, brochures, etc.)

Management support and reinforcement (e.g., presentations, meetings, etc.).

The responsibility of cyber security falls upon each and every individual within an organization. Today's hackers often target system deficiencies and software exploits, but the most effective method to interject viruses and gain access to protected information is perform by targeting personnel though email or social media. Hackers will often target personnel through "phishing" attacks and gain access after the user has opened the infected attachment or accesses a malicious website. OPPD has continued to defend against these highly crafted planned attacks by implementing a very robust cyber security awareness program. Annual training within interactive scenarios, consistent cyber security related articles posted on OPPD News, cyber security related posters and OPPD's SHIELD newsletter are a few of the methods used to strengthen OPPD's stance on protecting the organizations cyber assets.

For more information on OPPD's cyber security awareness program please visit the OPPD Cyber Security Awareness site.

If you have any questions or require any additional information regarding OPPD's Cyber Security Awareness Program please contact K.C. Carnes, Manager of Cyber Security and Information Protection, kccarnes@oppd.com. For questions regarding OPPD's NERC CIP Program please contact Michael Nickels – OPPD Reliability Compliance Specialist.