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

It's National Cyber Security Awareness Month

Each October, cyber security organizations observe National Cyber Security Awareness month as part of a combined effort to keep computer users mindful of the very real threat posed by cybercriminals and nation states. This October marks the 10th anniversary of this cyber security awareness campaign.

According to StaySafeOnline.org, over the past 10 years, the Internet has tremendously grown from 812 million users to 2.7 billion users. It's expected that by 2017 there will be about 3.6 billion Internet users, which should be about half of the projected world's population by then.

StaySafeOnline.org statistics show that during the past ten years the number of monthly active Facebook users has risen from 6 million in 2006 to 1.15 billion users. Yet during the same time, four out of ten social network users have become victims to social media based cybercrimes. One out of six social media users have reported that someone has hacked into their accounts and pretended to be them.

According to StaySafeOnline.org, during 2012 – 2013 an estimated 37.3 million users worldwide were subjected to phishing attacks, representing an 87% increase from the previous year (2011 – 2012). Small businesses have not escaped the scrutiny of cybercriminals, with an estimated 50 percent of all targeted attacks aimed at businesses with fewer than 2,500 employees.

StaySafeOnline estimates that the number of cybercrime victims has risen to 556 million per year. That's about 1.5 million victims a day or 18 victims per second.

"Today our nation's cyber networks are as much a part of the American homeland as they are indispensable to modern life in America – the very backbone of our 21st century economy and a major nerve center of our national security," Secretary of Homeland Security Jeh Johnson said in remarks supporting the National Cyber Security Awareness Month. "Cybersecurity is a shared responsibility," Johnson said. "Every one of us must practice basic cyber security because an intrusion into one computer can affect an entire network."

DHS has also stated, "The Internet underlies nearly every facet of our daily lives and is the foundation for much of the critical infrastructure that keeps our Nation running. The systems that support electricity, financial services, transportation, and communications are increasingly interconnected.

"By working together, we can rest assured that our homes and businesses will have power, our transportation systems will get us where we need to go, and our communication systems will help us connect at work and at home.

Just as critical infrastructure is essential to helping Americans live their everyday lives, a growing "Internet of Things"—the ability of objects and devices to transfer data—is changing the way we use technology and helping people live more efficiently. The Internet of Things encompasses the devices that are embedded with computers and, through a combination of sensors, connectivity to the Internet, and human activity, work to connect our lives to the digital world. Simply put, we are connected and online 24/7 even when we're not at a computer.

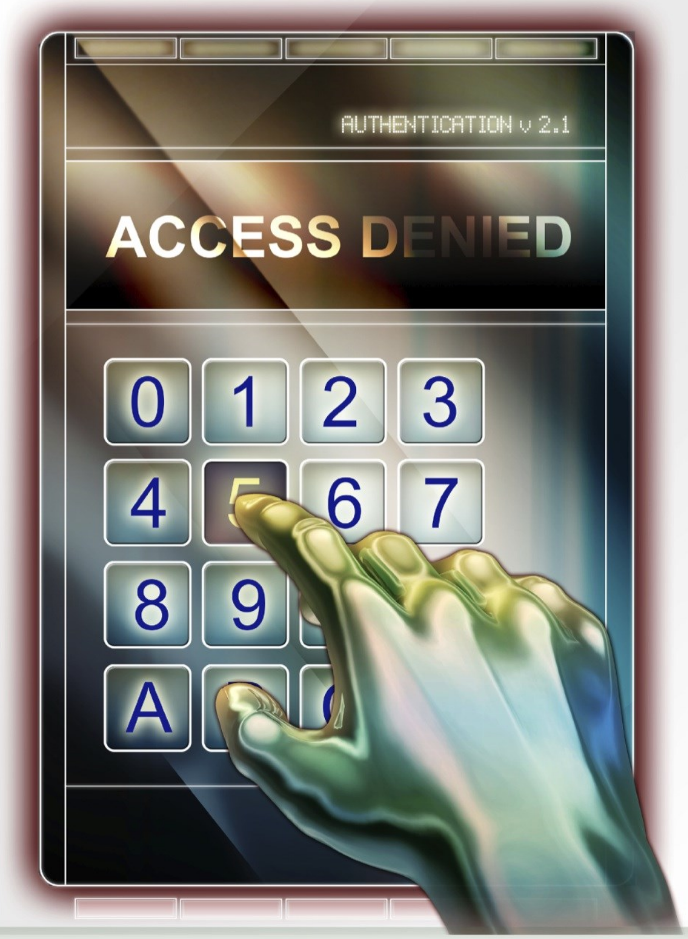
"Consumers play an important role in securing critical infrastructure not only by practicing good cyber hygiene themselves, but also by encouraging the many companies and organizations they do business with to adhere to high cybersecurity standards.

"By working together, we can protect the critical infrastructure on which we all we rely, keeping ourselves, our families, and our communities safer and more secure."

Passwords

Your passwords are the keys to your kingdom. Guard them well.

- The longer your passwords are, the better.
- Never share your passwords.
- Use different passwords for different accounts.



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

Be a Cyber Security Prepper

This year OPPD's Cyber Security and Information Protection team is reminding employees and contractors to take seriously the very real threat posed by cybercriminals and those interested in disrupting the nation's power grid.

Prepare for cyber security attacks by following these guidelines:

- Set strong passwords and don't share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates. This includes frequently exploited third party software found on home computers, such as Adobe Reader, Adobe Flash Player and Oracle Java.
- Talk with your family, friends, and community groups about Internet safety.
- Limit the amount of personal information you post online and use privacy settings to avoid sharing information widely. Anything you share will be used against you and others.
- Be cautious about what you receive and read online no matter how alarming or good it sounds. If it's too good to be true or causes you anxiety, it is likely to be bogus.
- Trust your friends but not their emails. If the email is unexpected, it may be a phishing attack.
- Do not respond to suspicious emails or links, even to opt out of unsolicited emails, instead, OPPD employees and contractors should report them to the Information Technology Service Desk.

Watch Out for Suspicious Email and Seasonal Scams

During Cyber Security Awareness month, we are revisiting topics that all computer users should know. As more and more of our communication and correspondence occurs online, it becomes increasingly important to be cautious when reading email. When you see an email from a strange or alarming source do not respond, click on any embedded links, or download any attachments.

We regularly spot email messages with very short messages bodies but with an attachment name containing a word like "invoice" intended to get a response from the user.

Users should also be aware that malicious content can also come from their friends and family. A user's account can be compromised and their address book used to target other users. Here are some questions to ask when reading the message:

- Do you regularly correspond with the email sender?
- Is the message out of character for the person?
- Is the message confusing or unsolicited?

Should any of these questions or other indicators raise any red flags, trust your instincts.

If your best friend suddenly has a large inventory of iPads or a story of some new miracle product, take a moment to think. If you are not completely sure whether the email is legitimate or not, call or text them to verify.

With the holiday shopping season fast approaching, be aware of seasonal phishing scams offering popular gifts at unbelievable prices. Bogus shipping notices also appear in greater numbers.

Other examples of seasonal scams include:

- Requests to wire transfer money (stranded traveler scams)
- Credit card application forms
- Fraud alert notifications
- Requests for charitable contributions
- Holiday-themed downloads (screensavers, e-cards, etc.)

If you receive any suspicious emails at work, make sure to report them to the IT Service Desk.

North American Electric Reliability Corporation (NERC)

Quarterly Update

OPPD’s NERC CIP Cyber Security Policy

CIP-003-3 R1

OPPD’s NERC CIP Cyber Security Policy represents OPPD’s commitment and ability to secure NERC CIP related assets and cyber assets. As required by NERC, OPPD’s NERC CIP Cyber Security identifies OPPD’s responsibilities pertaining to security and compliance actions in relation to the following NERC CIP Requirements:

Cyber Security - Critical Cyber Asset Identification, CIP-002

Cyber Security – Security Management Controls, CIP-003

Cyber Security – Personnel and Training, CIP-004

Cyber Security – Electronic Security Perimeter(s), CIP-005

Cyber Security – Physical Security of Critical Cyber Assets, CIP-006

Cyber Security – Systems Security Management, CIP-007

Cyber Security – Incident Reporting and Response Planning, CIP-008

Cyber Security – Recovery Plans for Critical Cyber Assets, CIP-009

OPPD employees and contractors with authorized NERC CIP Access can locate a hard copy of the OPPD NERC CIP Cyber Security Policy in or around NERC CIP Physical Security Perimeters. For OPPD employees, the OPPD NERC CIP Cyber Security Policy is located on the Cyber Infrastructure webpage page of the OPPD intranet. Finally, all OPPD authorized personnel who have completed the required annual NERC CIP Security Training are required view and adhere to all requirements identified within the OPPD NERC CIP Cyber Security Policy.

OPPD’s NERC CIP Cyber Security Policy is annually reviewed and approved by OPPD’s Vice President of Energy Delivery and Chief Compliance Officer, Mr. Mohamad I. Doghman.

OPPD’s Reliability Compliance Department recommends that all OPPD employees and OPPD contractors with authorized NERC CIP Access be familiar with this policy and to reference the policy for any questions or concerns there may be relation to OPPD NERC CIP assets and cyber assets.

References:

North American Electric Reliability Corporation (NERC) – Cyber Infrastructure Protection (CIP) Standards: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Midwest Reliability Organization: http://www.midwestreliability.org/

If you have any questions or require any additional information regarding this subject please

contact Michael Nickels – OPPD Reliability Compliance Specialist, manickels@oppd.com.