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

Phishing Email Is the Modern Pandora's Box

Opening a link or attachment from a suspicious source is very similar to opening Pandora's box. In the classic Greek myth, Pandora was given an attractive wedding present that she was never to open. Pandora was curious and released evil into the world. We experience this dilemma every day when scanning through our inboxes. A subject line catches your eye, the message seems believable and you can't help but open a link.

Here are some tips on what you should look out for when opening an email:

Does the sender email address match up with the alleged sender? Does it look like a legitimate email address? Sometimes, accounts can be hijacked and used to send emails, which you will have to use other methods to investigate. There are times when emails do not match who they claim to be.

Are there promises of money or gifts after your initial investment? Free money typically doesn't fall into your lap.

Are there requests for personal or account information? Companies should never ask for any account information through email. If it asks you to verify any information, follow up with the company's customer service that is provided on their official website.

Does the email just seem "phishy"? If you are suspicious for any reason, stop and research. If you are at work, you can send it in to the IT Service Desk for more research to be done. At home, you can research the company or the text in the message to see if anyone else has gotten it. If you receive a strange email from a friend, contact them using a different medium and verify whether they sent the message or not. A little research goes a long way.

These are just a few basic tips on how to spot phishing attempts. There are numerous resources on the internet that can educate you on what to look out for. Learn everything you can to avoid being a modern Pandora, releasing malware into our networks.

Image is based on painting by F S Church courtesy Wikimedia Commons.

Use Email Safely

Email is the number one method cyber criminals use to attack their victims. Be suspicious of odd emails or emails that seem too good to be true.

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

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.