



Phishing: Our #1 Threat

APPA Midwest Regional Municipal Cybersecurity Summit
Lourdes Herling, Ed.D.
Corporate Cyber Security Manager
Nebraska Public Power District

Recent Headlines

- [Baltimore Star, University of Maryland, 9/20/2019](https://www.foxnews.com/tech/2019/06/18/legislators-approve-sie-hack)
 - “The legislative reporter’s (Sie) has been a classic phishing scam. His email work for people in general on accounts was hacked last month and used to spam others with phishing emails.” (infosecurity-magazine.com, June 18, 2019)

Phishing Statistics

- 94% experienced a phishing attack¹
- 71% experienced an attack that spread to other computers¹
- 88% experienced email-based spoofing of business partners or vendors¹
- 73% of Business Email Compromise faced a direct resulting loss¹
- 94% of malware was received by email²

1. *The State of Email Security Report 2019 – Mimecast*

2. *Verizon 2019 Data Breach Investigations Report*

NPPD's Efforts

- Warning banner

This email is from bpouliot@publicpower.org. Do you know them and are you expecting this? - Look again!
Use the "Report Phishing" button if you think this is a phishing email.
Phishing is the #1 threat to NPPD. You are our best defense!!
Stay Vigilant!

- Link domain

<https://tecuseh.filecloudonline.com/url/7higehp266piymid> [od.lk]

- Report Phishing button



Phishing Examples

PO - Message (HTML)

File Message Help Tell me what you want to do

ED

Wed 4/10/2019 9:09 AM

PO

To

If there are problems with how this message is displayed, click here to view it in a web browser.

adobeinvoice-com.firebaseio.com

For questions or comments, please feel free to contact us.
Regards!

-----Original Message-----

From: mfdscan

Sent: April 10, 2019 6:16 AM

To: Don Edwards

Subject: Scanned from a Xerox Multifunction Printer

Intuit Quickbooks <intuit-quickbook-billing@xero.com>

To

Invoice Due: 05/06/2019
17340

Amount Due: \$9,548.00

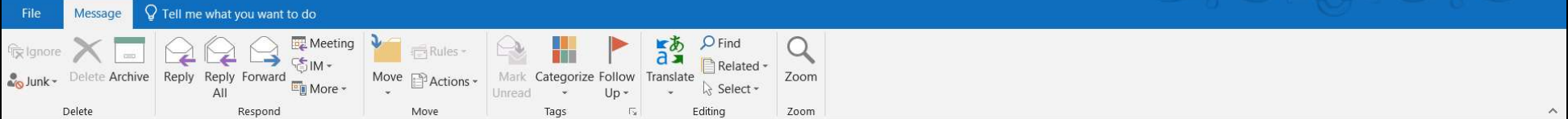
Dear Customer:

Your invoice is attached. Please remit payment at your earliest convenience.

Thank you for your business - we appreciate it very much.

Sincerely,
Accounts Receivables
813-170-7236

[ganeshshree.com]



no-reply@onedrive.com n Onedrive. Tue 9/11

Th salesforce@digitalpromotioninc.com pecting this? - Look again!
ail.
Phishing is the #1 threat to NPPD. You are our best defense!!
Stay Vigilant!

[_sharepointOnline_](#)

5kgpghrm-yfpc081a03njg&r=xcvwdfi1lkwa0
zqbmlk_sw&m=81hbmyh5gvnloaag_1rlgit_
0vwpfcfdnaizezdxas&s=jc9yibjcol6vt5ennx
vektrdhijrfyy28fi7qak1ry&e=
Click or tap to follow link.



A Microsoft OneDrive notification card. It features a PDF icon, the text "Hello p**ope@nppd.com", and "A file has been shared with you on SharePoint." Below the text is the Microsoft OneDrive logo. A red arrow points from the URL in the previous block to the "p**ope@nppd.com" text in this card.



Wed 5/15/2019 12:22 PM

You Just Received a File from [REDACTED]

To: mail@pop.com

This email is from [REDACTED]@tecumsehne.com. Do you know them and are you expecting this? - Look again!
Use the "Report Phishing" button if you think this is a phishing email.
Phishing is the #1 threat to NPPD. You are our best defense!!
Stay Vigilant!



[REDACTED] has shared files with you.

Tecumseh Invoice_324722 Claims - Docs.pdf

at <https://tecusehfilecloudonline.com/url/7hiqehp266pivmid> [od.lk]

[REDACTED] has also sent the following message:

You've received a document awaiting your review.

Thanks.

Click on the link above to access your files.

You received this message because you signed up for an account at FileCloud.

w-9 &.pdf
572 KB

General New remit info Bank of America .pdf
162 KB

From: Scott Fitzgerald [<mailto:sfitzgerald@generalexexcavating.com>]

This email is from sfitzgerald@generalexexcavating.com. Do you know th

Use the "Report Phishing" button if you think th

Phishing is the #1 threat to NPPD. You are

Stay Vigilant!

Kindly be advised that due to changes in management and new developments in General Excavating Company, we have now updated our remittance information. Hence all due payments and All future payments should be remitted to our updated banking information and check information as soon as possible. Please see attached Letter and updated W9 for more Elucidation .

Scott Fitzgerald
President

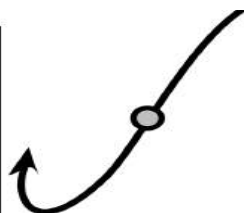


706.309.2598 phone | 402.467.2084 fax
GENERALEXCAVATING.COM [generalexexcavating.com]

[Facebook](https://www.facebook.com) [[facebook.com](https://www.facebook.com)] | [Twitter](https://twitter.com) [twitter.com] | [LinkedIn](https://www.linkedin.com) [[linkedin.com](https://www.linkedin.com)]

NPPD Awareness Training


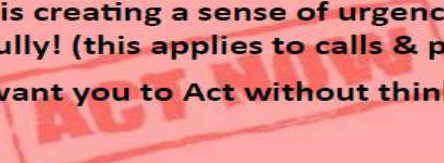
- Monthly phishing simulations
 - Baseline for each type
 - Increasing difficulty
- Presentation at Quarterly safety meeting
- Advanced training for Executive Assistants
- October National Cyber Security Awareness Month
- Quarterly posters
- Monthly articles



When it comes to **Phishing**

Consider all the **FACTS**



F rom	Who is the email From? Have you received emails from this sender before? Beware of attackers spoofing trusted individuals or companies.
A ction	What are you being asked to do? Are you being asked for protected information? (username, password, SSN, etc.) What does a potential attacker stand to gain?
C ontent	Are there links? Do they go where you expect? Beware of attachments you weren't expecting. Check all shortened or obfuscated URLs before clicking. (ex: bit.ly links) 
T one	If an email is creating a sense of urgency, Stop and Look Carefully! (this applies to calls & pop-ups too) Attackers want you to Act without thinking. 
S ense	Does the email make sense? Is the email you received part of a routine/scheduled communication? If you don't need it, <u>Delete It!</u> 