COMPUTER CHRONICLES

PowerManager®

Efficiency through utility business management software

NMPP ENERGY — SALT CREEK SOFTWARE, INC.

Phishing attacks remain top cyber threat

By David Russell, CGCIO
NMPP Energy

Phishing remains a top cyber threat throughout the world. Phishing is involved in 36 percent of breaches according to the Verizon Data Breach Report (DBIR) 2021. Also stated in the same report:

• The median loss of a Business Email Compromise was $30,000

• 95 percent of Business Email Compromise losses were between $250 and $984,855

• 85 percent of breaches involved the human element

• 35 percent of breaches in North America involved social engineering

• Social engineering pattern was responsible for more than 69 percent of breaches within public sector

• Almost 100 percent of social attacks in the public sector involved phishing

• 96 percent of social attacks arrive via email

The phishing email itself is usually just the beginning of an attack and opens the door to others:

• **Credential phishing** helps attackers capture and use stolen credentials to access sensitive systems or data appearing as if they are legitimate users.

• **Malicious files and URL links** allow attackers to spread malware that helps steal data and or encrypts it potentially causing a significant loss to an organization. Many of these attacks lead to ransom demands to get your data back and there is no guarantee that you will get the data back if the ransom is paid.

• **Impersonation attacks** make emails look as if they are coming from a legitimate sender. By imitating someone's name or email it will trick you into providing sensitive information or clicking a (URL) to launch malware.

DID YOU KNOW?

POWERMANAGER SOFTWARE IS USED AT 180 LOCATIONS ACROSS THE U.S. AND BEYOND

POWERMANAGER IS USED IN ARKANSAS, COLORADO, KANSAS, INDIANA, IOWA, MASSACHUSETTS, MINNESOTA, NEBRASKA, NEW YORK, NORTH DAKOTA, OKLAHOMA, SOUTH DAKOTA AND HONDURAS.

PowerManager®

Welcome new PowerManager users!

The PowerManager family welcomes:

• City of Yutan, Neb.,

• Village of Guide Rock, Neb.

• Village of Wynot, Neb.

• Otoe County Rural Water District #3 in Syracuse, Neb.

**2022 PMUG
Annual Conference**
Sept. 14-16, Best Western Plus, Bloomington, Minn.

**2022 PowerManager
Training Sessions**

Oct. 5-6, NMPP Energy Building, Lincoln, Neb.(In-person and virtual)

Dec. 14, End of Calendar Year Reporting - Virtual 1.5-hour Training Session.

IRS mileage rate to increase July 1

The Internal Revenue Service recently announced there will be a mileage rate increase effective July 1. This increase will be from 58.5 cents to 62.5 cents per mile.

Phishing attacks
cont. from pg. 1...

Identifying phishing email can be tricky. Typically, you can identify them due to misspelling and grammatical errors. However, phishing emails are getting more sophisticated and are becoming much more difficult to determine if they're legitimate. To help spot these phishing emails as a user, you need to review various aspects of the email before you click on anything in the body or open any attachments. Here is an example of a phishing email that appears as if it is coming from NMPP Energy.

Using the email example at right, look out for the following:

1. The domain that it is coming from – it is coming from Gmail, but it is supposed to be coming from nmppenergy.org, not Gmail.

2. It is asking for sensitive information that should not be asked for in an email like this
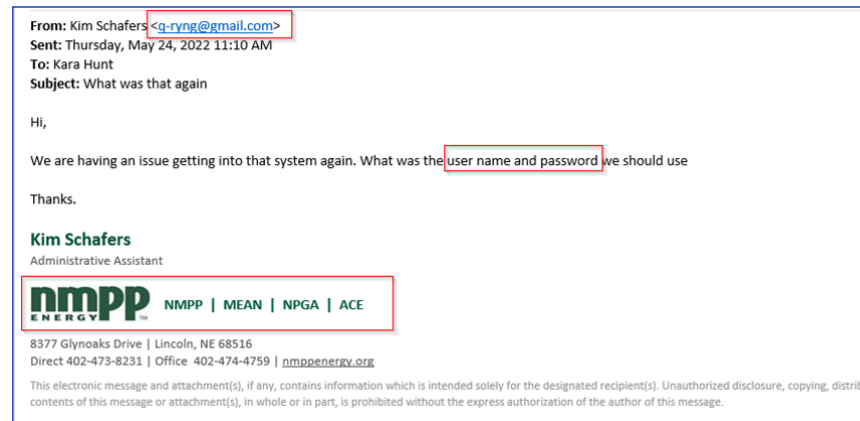
3. The email is using an OLD company logo.

Always look for inconsistencies in emails before you reply, click on a link or attachment. If you are in doubt on the legitimacy of an email, call your IT department or the person you are supposed to have received the email from to ensure that the email is valid. Taking a few extra moments to review the email to ensure its validity can save an organization a significant amount of money and time.

There are various ways an IT department can implement tools to help identify and mitigate phishing email such as email content filtering, email authentication, and threat intelligence. One of the biggest ways an organization can help mitigate the risks associated with email phishing is to conduct phishing campaigns and awareness training for its users. If you need help in this area or have any questions, please reach out to us, we are always happy to assist.

PowerManager Error 6610 explained...

PowerManager Error 6610, The Advantage Database Server Did Not Respond to a Database Request in a Timely Manner.

This error typically is returned by PowerManager after it was not able to communicate with the Advantage Database Server (ADS) and timed out the connection the workstation had with the ADS as a result.

The most common cause for this error is your workstation went to sleep. When it goes to sleep, PowerManager may still be running, but your workstation is not continuing to send packets to the ADS, causing the connection to timeout. By the time you wake up your PC, PowerManager has lost the connection and generates the 6610 error.

To avoid this error do not put your workstation to sleep and ensure that it is not set to sleep automatically
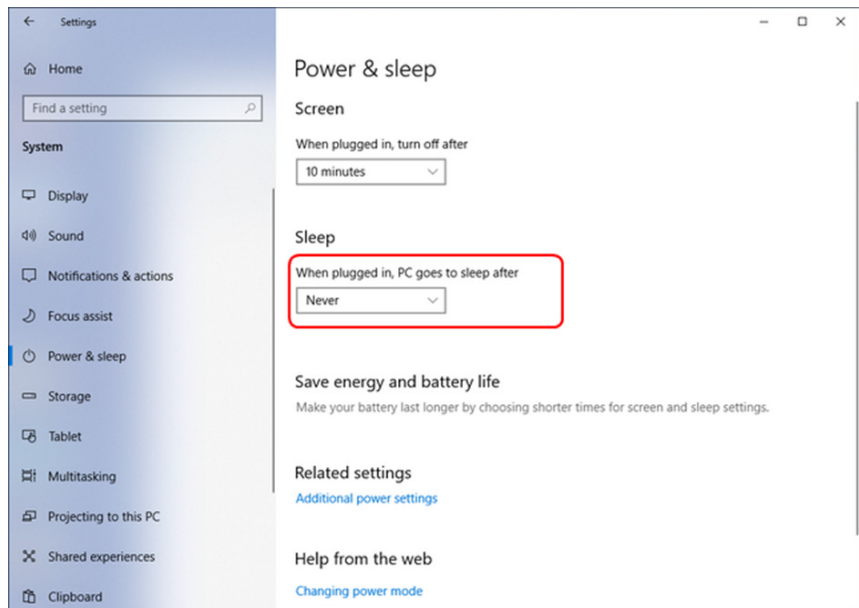
 Windows Start button

 Windows Settings button

after a period of inactivity. Instead, lock your workstation. Alternatively, make sure you've completely closed out of PowerManager before allowing your workstation to go to sleep.

To review your workstation's power and sleep settings click on the Windows start button,

typically found in the lower left-hand part of your screen, then click settings. The settings button is typically the second item straight up from the Start button. From the settings screen click on "System" then "Power & sleep". Make sure the value for "When plugged in, PC goes to sleep after" is set to "Never".