HACKERS, PHISHING, AND OTHER NASTINESS

Be alert and aware of efforts by hackers to access your office computer systems. Hackers are attempting to gain access to systems around the world. Recent reports indicate that hackers have gained access to email accounts of government officials in systems we would all assume have an elevated level of security.

Be sure that you take all necessary steps to protect your systems. Activate a strong firewall, install anti-virus software on your computers, devices, and hardware. If you can afford it, engage an outside consultant to help install and evaluate the methods you use to protect your systems and the information they contain.

Many hacking incidents are not due to hackers penetrating a firewall; rather, hackers send emails to employees that appear to be legitimate. This is known as phishing. Recipients click on links or attachments in the emails that infect their computer or device. The malware or virus may spread to other PCs and servers to which that computer is connected. "Spear phishing" is a more targeted form of phishing in which the sender poses as a trusted person, such as a family member, and tries to get the recipient to act based upon that trust.

Phishing is based on social engineering, which is psychologically manipulating people into performing actions (ex. clicking on links or attachments, transferring money to hacker-held bank accounts) or divulging confidential information (ex. social security numbers, bank account information).

Councils and sessions should encourage all of their employees to do the following:

1. Be extremely cautious of unsolicited email, no matter the source. Phony emails can look like they come from family, co-workers, session or council members, government agencies, banks, or legitimate businesses. Employees should not randomly click on links in emails or open attachments until they verify that the email is legitimate. Recent reports indicate that AI (artificial intelligence) is making it easier for bad actors to phony up business emails that look genuine, as if coming from a supervisor, with links that lead to insertion of malware or ransomware, or the sender asks recipients to transfer sums of money to accounts controlled by the bad actors.

2. Sometimes family or friends will have their home email systems hacked and the malware/virus installed in those systems by bad actors will find the address book and send emails to everyone in it (including your employee). Messages will be short, something like, "hey, check out this cool YouTube cat video" with a link. Employees should not click on that link! They should call the sender and ask if the sender sent the message. It is just another example of social engineering and manipulation. A relative appears to send a desperate email, "we are on vacation and all our money was stolen, please help and send us money." The bad actors learned the sender is on vacation from a Facebook post, so the recipient may be persuaded that the email is legitimate. Best practice is to delete messages if they are not work related (no offense to cats, but you can Google pet videos on your own time). Employees should tell family and friends to send personal emails to the employee's home email address; let us keep personal and work emails separate.

3. Government agencies and banks will not send employees emails! They will mail them letters or appear at their door with a subpoena. If they get an email at work from the IRS or the FBI, they should not click on links or attachments; they should contact the agency that allegedly sent the email and ask for help. They can also use the internet to search for information on scams. For example, the FBI has good advice on online safety and security: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/on-the-internet and has a page they can search for information on scams: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety .

4. If an employee gets an email asking them to pay a bill, provide a password or click on an invoice, the employee should be extremely cautious! Hackers are sending such emails hoping the employee is busy and concerned about paying bills and they will not pay attention; they will just click on a link to view an invoice or pay one. For example, the phony emails will say something in the subject line such as ATTN: Invoice No. 245-G-123 and in the body it will say "please review the attached invoice" or

"please click on this link to review the invoice" or "your payment is past due, and your account may be cancelled." This is a trap, more social engineering, it is a construct to get the employee to be nervous about the alleged overdue payment, so they immediately react and click rather than verifying. Encourage employees to take time to verify that such emails are legitimate. They should contact the sender. Also, they can hover their cursor over the sender's email address and see if it appears to be from the company that claims to be the sender. In the end, the employee should verify before clicking.

5. If employees get an email asking them to forward W-2 forms or personal information about themselves or co-workers, they should verify the request before responding. This is phishing. They should contact the person who allegedly sent the email (ex. Chair of Personnel Committee) and ask if the email is legitimate. If so, then, and only then, respond.

6. No one is going to email an employee to offer the opportunity of a lifetime (congratulations, you just won a lottery for which you did not buy a ticket and your winnings are in a foreign country and if you send us a few thousand dollars through Western Union we will release your millions of dollars in winnings!). If employees get such an email**,** they should delete it.

7. If employees get a screen that tells them that their files have been encrypted and are being held for ransom, they should immediately disconnect their computer or device from the system by disconnecting the wires from their computer. The employee should contact the Head of Staff about engaging the services of a digital consulting firm for help, and notify the FBI, via the Internet Crime Center. https://www.ic3.gov/

All employees must be vigilant to protect your systems and the documents and information they contain. Talk about best practices with office staff and practice smart email safety, encourage employees to question and verify requests for money or personally identifiable information and to avoid automatically responding to emails no matter how legitimate they may appear to be.