CALIFORNIA RURAL WATER ASSOCIATION
MEMBERGUARD
Serviced by Glatfelter Public Practice

RISK COMMUNIQUÉ

A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

Cyber Security – Email Phishing Precautions

Email has evolved into a mission critical business function for many organizations and for this reason, it has also become the primary mechanism used by Cyber Criminals to gain access to protected systems. One of the primary methods used by these criminals is a simple technique called "Phishing," which is an attempt to acquire sensitive information by masquerading as a trustworthy source.

The term phishing was coined by hackers in the 1990s in reference to their process of using email to convince recipients into giving up their passwords or financial data. Times have changed and the phishing attempts have become widespread and extremely sophisticated.

Malicious components of a Phishing Email

- Attachments – A file (Microsoft Office document, pdf or image file) attached to the email will contain malicious software called malware. Upon opening the attachment, the malware attempts to infect the machine or reach out to the Internet to download additional malware to the system.
- Embedded links to websites – The embedded link will appear to take recipients to a legitimate website. However, they will be redirected to a fake site that attempts to collect credentials and then pass recipients to the legitimate site. Many times, these fake sites also attempt to install malware onto the system.

Malware can be used to provide remote access to your system, steal information or even encrypt (make unreadable) the files on your computer and hold them for ransom (called ransomware).

A recent study performed by Google and the University of California, San Diego, identified some interesting statistics[1] from phishing attempts against Google/Gmail:

- 35 percent of phishing sites attempted to collect email credentials.
- 21 percent of phishing sites targeted banking credentials.
- An increasing number of sites are targeting social networking credentials.
- 20 percent of stolen Google credentials were used to gain system access within 20 minutes of the account being stolen.
- When an email account is taken over, the email history and address books are searched to determine how to best utilize the account.

McAfee Labs Threat Report[2] also found that 80 percent of individuals who participate in their McAfee Phishing Quiz (phishingquiz.mcafee.com) have fallen for at least one in the seven phishing emails.

[1] "Handcraft Fraud and Extortion: Manual Account Hijacking in the wild" by Google, Inc. and University of California, San Diego. 2014.

[2] McAfee Labs Threats Report. August 2014

Tips for identifying a Phishing Email

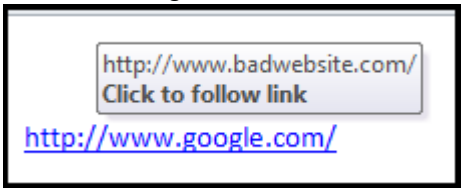
Not all phishing emails can be easily identified, but there are some basic attributes that can be used to raise the suspicion level of an email. If any of the statements below are true, delete the email or use extra caution before opening:

- Not recognizing the sender of the email.
- The email is asking for personal or financial information.
- The email wants the recipient to respond immediately or makes an urgent request for information.
- The email includes upsetting or exciting statements, which are usually false, that want the recipient to act quickly.
- The email wants the recipient to open an attachment or click on a website link that was not expected. This could be to view an article or video pertaining to any number of intriguing topics such as current social events, news tragedies or holiday sales. Other forms include a notification of fraudulent charges on a credit card, or a cell phone or email account has been locked out.

Email safety tips

The easiest way to avoid falling victim is to delete any emails that can be identified as suspicious. If the email looks legitimate or is from a valid sender, there are several safety tips listed to follow:

- Never send financial or personal information (account numbers, social security numbers, credit card numbers, ID's and passwords, tax identifier numbers, etc.) via email unless a form of email encryption is being used. This is a special type of email that scrambles the information so only the recipients can read it.
- Verify that website links embedded in emails are being directed to the correct website Do this by placing the cursor over the link (do not click on the link). Hovering over the link will show you the real website in a pop-up window or if using a web browser it will be in the lower left hand corner.



- Contact the sender to verify that the email was legitimately sent to you.
- Instead of clicking on the link provided in the email. Contact the sending party to obtain their legitimate website and manually type it in to the web browser.
- Consider using separate email accounts. One for business, one for financial institutions, one for friends and family and one for subscriptions and registrations.
- Run firewall and anti-virus/anti-malware detection programs on computer systems. These are subscription-based services and it is important to keep them up-to-date.
- Use different and complex passwords for each account that utilizes email addresses. Using the same password across accounts will compromise accounts if the credential is stolen.
- Never reply to a suspicious email as this will validate your email address as active.
- When using hosted email services (Yahoo mail, Gmail, Outlook online, etc.) enable two-step verification. Once the password is entered, a prompt will ask to enter a randomly generated code that is sent to a mobile device.

Phishing emails can be very sophisticated and convincing. Those who fall victim to a phishing email, should take action immediately.

Phishing victim action plan

- Notify the IT department or vendor of the organization to enact any Incident Response Plans (IRP) that may be in place.
- Scan the system with an anti-virus or anti-malware product.
- Change any account passwords that utilized the compromised credentials.
- Monitor any compromised accounts for suspicious activity or fraudulent charges.
- If financial account credentials were compromised, notify the appropriate financial institution or organizational representative.