An InfoSec Update

The Tax Man Cometh…And So Do The Scams

Ben Franklin said: "There are only two things certain in life: death and taxes."

With apologies Mr. Franklin but there are three: death, taxes, and scams. The usual tax season cybercriminal activity is already underway. Phishing campaigns impersonating popular accounting and tax-filing software have already been spotted. Many of these campaigns threaten to close user software or tax filing accounts unless they "click the link" to indicate the account is still in use.

One tax software provider, Intuit, reported seeing emails purported to be from the "Intuit Maintenance Team". The email informs the recipient that their account has been "temporarily disabled due to inactivity". and that it is "compulsory" to restore access to the account within 24 hours. The email further states that "This is a result of recent security upgrade on our server and database, to fight against vulnerability and account theft as we begin the new tax season".

Spot the Scam: Think Before You Click:
Knowing the anatomy of a phish will help you spot and avoid the phisher net.

- Our culture has become extremely fast paced. Phishers are counting on us speeding through our emails. The number one reason for falling victim to a phish is rushing and not paying attention. Step one is SLOW DOWN with email. Take your time.
- The email may appear to be from a known or trusted source: Don't trust the FROM line. In most popular email applications, hovering your mouse over the name on the FROM line will cause a pop up to appear. This pop up displays the underlying email address for the message. This gives you a chance to validate that the sender is who they say they are.
- Phishing emails play on your emotions. They play on your hopes and fears. Get rich quick schemes or the "something bad will happen" scenario are the two most common.
- There will be a sense of urgency tied to the email. "Act Now!", "The offer expires within 24-hours" or some other time-based action is needed (as in the Intuit example above).

Protect Yourself By:

- Ensuring your operating system, applications software and antivirus programs are up to date.
- Follow the guidance on how to Spot the Scam, above.
- If you think it is a phish:
    - Don't forward it to others. If it is a malicious email, you risk spreading the danger.
    - Delete it.
    - Keep in mind that if it came from a legitimate business, you should be able to visit their web site and confirm the information. Barring that, you can always call the sender using a known good phone number to confirm the information.
    - If at any time you receive an email from PenFed that appears suspicious, forward it to abuse@penfed.org

Tax season can be scary enough without having to worry about being scammed. A little patience, some easy email detective work and you can be confident that you will make it through another Ides of March.

#BeCyberSmart
Remember, Security is Everyone's Responsibility

PENFED CREDIT UNION