Legal Services National Technology Assistance Project

www.lsntap.org

Webinar: Phishing

Phishing

In this webinar we look at what phishing is, why and how people do it, and what you can do to safeguard your organization against it. We go into more detail in the webinar but there are two core lessons to be learned. First of all it is not a matter of if, only a matter of when. The phishers attack targets ranging from individuals to large government organizations so you and your organization are within their sights. In addition while some of the attacks are relatively easy to spot some of them are tailored to their target and either way they send out huge waves of messages and only need a single mistake to take over a system. Secondly to prepare for an attack as an organization you need a variety of solutions involving technology and training. A well-educated staff can spot phishing emails as they come and will be empowered to ask for help if they are unsure or let IT know if they accidentally opened a suspicious email. On the other side an offsite backup that is regularly updated will turn an otherwise crippling attack that gets through into an annoyance.

https://www.slideshare.net/LSNTAP/security-session-on-phishing

I had gotten a little behind so today we have a double feature. First we have a webinar covering phishing from today followed by the language access for websites webinar from last week.

Who We Are

Michael Green, JustTech
Mike is a Technical Consultant & Engineer at Just-Tech with over 18 years of experience in the field of Information Technology, and works with clients on project planning and systems implementation. He also works as an engineer behind the scenes.

Mary O'Shaughnessy, Her Justice
Mary has long experience in for-profit and nonprofit technology services, including technology audit. She has been Director, Information Services at Her Justice since 2012.

What is Phishing?

An attempt to bait a user into giving up sensitive information or to otherwise provide access to their system.

Why are they doing this?

Their end-game is $Money$!

Most common methods to accomplish:

1. Compromise systems and key user accounts who have control over finances and move money covertly themselves.
2. Hold systems and/or data hostage for a ransom payment.

Impact

- Access to CMS- client information & disclosure rules
- Access to internal files- ID theft & personal info
- Damage to reputation/community relationship
- Increased recovery cost if unprepared
- System downtime

The Phisherman's Bait

- Disguised to mislead- FedEx/Invoices, Client Assistance/Urgent Emails
- Can be personalized (Spear Phishing) (Whaling: targeting top executives)
- Password Reset phishing/Fake communications from IT
- URL manipulation - falsifying hyperlinks
- Attachments with malware

How to recognize it?

Though the Phishers are deceptive in their tactics, there are tell-tale signs of fake information.

1. The email is threatening, provoking, or pretends to be authentic correspondence, in an effort to get you to open attachments or click links on impulse. Phishers need you to "take the bait" and allow them in.
2. The actual sender's email address does not match who they claim to be.
3. Mouse-over hyperlinks reveal sketchy website destination.
4. Porr sppelling or errors grammatical.
5. Sender claims to be internal, popular, or reputable source.

Technology Prevention

- Keep systems & antivirus updated and enabled
- Have measures in place (disable URLs/scan attachments where possible)
- Reliable Backups and Recovery Plan
- Cyber Insurance

Human Prevention

- Check with IT for verification **before** action
- Ignore unsolicited email links & attachments
- Continual Training & “Cheat Sheets” for staff
- When in doubt, Ask about
- Add to Junk Mail list

Policies/Training

Policies - Acceptable Use, Mobile Device, Guest Use, & Email policies are just a few

New Staff/Veterans/Volunteers - Whether they started yesterday or 20 years ago, continual training and coaching is a necessary component to prevention. Viruses and Malware continue to evolve, we need to adapt as well

Training Practice - https://www.phishingbox.com/

US Computer Emergency Response Team tips - https://www.us-cert.gov/ncas/tips/ST04-014

Helpful Resources

- LSNTAP-lsntap.org
- Idealware- www.idealware.org
- Security Awareness Training-www.travelingcoaches.com
- YouTube Videos- While not tailored, can provide self-help
- Resources on corporate identity theft- https://archives.fbi.gov/archives/news/stories/2007/june/idtheft_061807
