Phishing: Don’t take the bait!

|

Rob Tompkins, CISSP, Lead Cybersecurity Engineer, Tulane IT Information Security Team

View PDF

When you open your email, you probably see endless ads, responsibilities, and links to funny cat videos.

When an attacker sees your inbox, they see a potential goldmine.

You may be familiar with the term “phishing.” Phishing emails are designed to trick you into giving away information about yourself or your company.

Quick history lesson: In the year 2000, a phishing email was sent with the subject: ILOVEYOU. Known as the Love Bug, users were invited to open an attached “love letter” which showed no love at all. Rather, it was a worm that deleted files and sent the same email to the user’s contacts. It is estimated that **45 million Windows PCs were affected by this attack** (and countless members of the workforce were heartbroken that their co-worker didn’t ACTUALLY love them)! Phishing emails are the top method attackers use to get initial access into a network.

A lot has happened since then. The goal of phishing remains the same, but it’s not just about your work computer anymore. Attackers are now correlating personal email addresses to the person’s place of business and attacking that business with a personal email. We’ve also seen the rise of voice call phishing (known as vishing) and SMS or text message phishing (known as smishing). Coupled with the rise in mobile device malware and the fact that most users can access email inboxes on their phones: it is a recipe for disaster.

If you ask any information security professional what keeps them up at night, most will say ransomware. If they don’t, they’re lying.

Ransomware is malware that requires the victim to pay a ransom to access encrypted files and is usually spread through phishing emails.

The University of Vermont Medical Center (UVM Health) underwent a ransomware attack in October 2020. Because most organizations are implementing tools to block phishing emails, the group that attacked UVM Health sent the email to an employee’s personal email. This will sidestep most of the security tools in place. Once the user clicked on the link in the email, it installed ransomware on that machine and then spread to the rest of the network, infecting 5,000 computers. It shut down the entire network. Estimates put the damage at $63 million, and the effects are still felt today.

No one wants to be “that person” who clicked on the link and shut down the entire network, so how can we protect ourselves?

Phishing Tips

There are a few key things you can do today to protect yourself and the Tulane community:

1. **Enable MFA.** Multi-factor authentication (MFA) makes it harder for cybercriminals to access online accounts. Enable MFA whenever it is available for an online account. We use DUO at Tulane.
2. **Remember the phrase SLAM.** This acronym reminds you to check four things when you see a suspicious email or text:
    1. **Sender**: Do you know the sender? Is it someone you have contacted before?
    2. **Links**: Hover over the link to view where it goes. Don't recognize the URL? Don't click on it.
    3. **Attachments**: Attachments can hide malware, even PDFs. If you don't know the sender or are suspicious at all, don't save or open the attachment.
    4. **Message**: Unusual grammar, spelling, and phrasing are a dead giveaway that the email may be from a cybercriminal.
3. **Always double-check before you click the link!**

Phishing is the number one way attackers gain access to your business accounts or personal information. If you have not been "phished" yet, it may just be a matter of time. Only by staying vigilant can you protect yourself, your identity, and the Tulane community from these cybercriminal attacks!