frogworks

2023

Issue 4 Volume 13

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Tips to Recognize and Avoid Phishing Attempts:

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as passwords, credit card numbers, or bank information -- on websites that pretend to be legitimate.

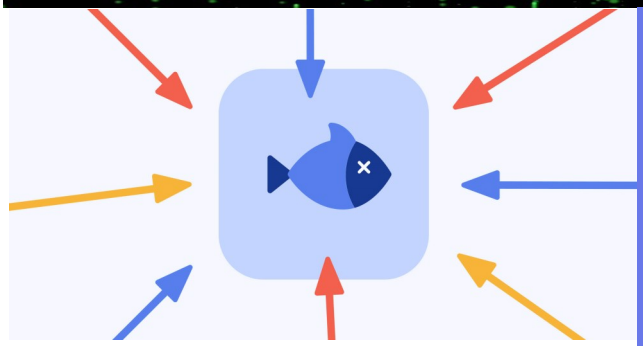
It really isn't all that difficult for a cyber-criminal to infiltrate your network. All they need to do is compose an email. It doesn't have to be very long or even that professional-looking. At this point, almost anything works… or, at least, that's what it seems like, since the total number and overall success rate of phishing attacks have both grown significantly over the last few years.

This fact is disappointing and frustrating to us because phishing emails can be easy to detect and easy to avoid. All it takes is a little suspicion and a few seconds of work to effectively sidestep a phishing attack. So, just to make sure you have absolutely no excuse to fall victim to a malicious email, here's a 5-part strategy to help you maneuver through your inbox.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Tips to Recognize and Avoid Phishing Emails :

- **1.Review the sender:** Before you open the email, take a look at who sent the email. Sometimes a malicious email can be stopped right here. Do you know who this person is and does it appear to be from a credible source? Oftentimes, a phishing email will come from an address that is clearly malicious in nature.
- **2. Review the subject:** If the sender doesn't catch you off the guard, then the subject line probably will. Malicious emails usually have ridiculous subject lines that appear to be urgent and time sensitive. If something like this comes from an unknown source, it's probably a bad email. Think about it: Why would someone you don't know send you an urgent request through email?
- **3.Inspect the grammar:** If you make it to the actual email itself, and the sender and subject appear to be legitimate, it's time to review the content itself. These emails should have correct punctuation and correct grammar. If something is grammatically off, delete the email. However, if it's coming from an individual person, you may need to be a little less skeptical here.
- **4.Take a look at the content, and contact information:** Once again, if the email comes from an actual company, make sure everything matches. Does the logo, header, and contact information match the company's actual getup or is something slightly off? If it comes from a person claiming to be with a company, they should have a signature with the proper logo and contact information to match the company.
- **5. Approach attachments, call to actions, and links with caution:** It's a good rule of thumb not to open anything or click on anything from an unknown sender. If it comes from your phone company or your banking institution and you aren't completely sold on the legitimacy of the email, then find a roundabout way of accessing the same information. If it's a call to action that asks you to update your login information by clicking on a link, then delete the email. Instead, type the normal website into the address bar, login to your account from the website, and update your account.



What is Spear Phishing?

- **Spear Phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to targeted individuals for the purposes of revealing confidential information (passwords or financial) or to install malware.**

How It Works: An email arrives, apparently from a trustworthy source, but instead it leads the unknowing recipient to a bogus website full of malware. These emails often use clever tactics to get victims' attention.

How To Spot Spear Phishing Attempts

- The clearest indication is if the email address does not match the name of the sender. It is free to create accounts in many places, and you can name them however you want, even if that name belongs to someone else. Now, free accounts like gmail.com, yahoo.com, and outlook.com aren't the only places to create emails, there are hundreds of ways to create and send an email, so make sure that the email is being sent from the correct domain.
- Next up is the information in the email. If the email claims that wiring instructions have changed, that a website needs to be opened, that account information needs to be verified, or anything else of this nature, then it has a high probability of being spam.
- Additionally, check the signature line. If you suspect that an email has been spoofed, check if the signature line matches up with another, verified email from that person. There could be a difference in font, wording, phone numbers, addresses, and even in the photos

The following two pictures are examples of this. On the left is a real signature line, and on the right is the signature line of a spoofed email. It has the same words, and even the same phone number but the formatting is wrong. Oftentimes, scammers will leave out the touches like the business' logo or any photos, and instead write everything in plain text.

Alex Bleam, Owner

For service, please call: 240-880-1944

#1 frogworks
Managing Your Technology So Your Business Doesn't Croak.
NEXTGEN 101

Office hours: 8AM-5PM, Monday -Friday

Thank you,

Alex Bleam

240-880-1944

Frogworks

Securing Your Credit Card Data:

• Check Statements Regularly

Don't wait for your bill to come at the end of the month. Go online regularly to view electronic statements for your credit card, debit card, and checking accounts. Look for any fraudulent charges, even originating from payment site like PayPal and Venmo. You should buy online with a credit card. If your debit card is compromised, scammers have direct access to your bank funds.

• Skip the Card, Use the Phone

Paying for items using your smartphone is standard these days and is even more secure than using your credit card. Using a mobile payment app like Apple Pay generates a one-time-use authentication code for the purchase that no one else could ever steal and use. You just need your fingerprint, face, or passcode to make it happen instantly.

• Look for the Lock

Never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed—at the very least. You'll know if the site has SSL because the URL for the site will start with HTTPS—instead of just HTTP. An icon of a locked padlock will appear, typically to the left of the URL in the address bar or the status bar down below; however it depends on your browser.

• Protect Your Computer

Swindlers don't sit around waiting for you to give them data; sometimes they give you a little something extra to help things along. You need to protect against malware with regular updates to your antivirus program. Better yet, pay for a full-blown security suite, which will have antivirus software, but also will fight spam, spear-phishing emails, and phishing attacks from websites (the latter two try and steal your personal info by mimicking a message or site that looks legit).

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures. Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER