PHISHING

venture POINTE
A TRUE Technology Partner
(904) 351-8101

Remember the days when all you thought about when someone said something about phishing, was heading to your favorite pond?

Well now that word has become synonymous with fear and strife in the workplace, as well as at home.

Always wondering if that email or email attachment is really a surprise UPS package or your favorite cookie recipe from your mom.

While Venture Pointe is ready and able to more than adequately protect your network and your data environments, even help install fail safe processes and oversight to protect against all types of hacks and attacks.

The one thing no one can fully stop are phishing based emails, those are preying on the unknowing, inexperienced, or maybe just someone in a rush.

What is Phishing exactly:

Basically, it is an attempt to get sensitive information from you such as passwords, usernames, or personal information.

How do they do that?

Well most attempt to trick the end user by pretending to be someone you trust, or something/someplace that you are comfortable with or deal with on a regular occasion.

You will receive an email, IM message or really any form of online communication sometimes suggesting you have some sort of issue needing resolution; examples would be password reset request, account confirmation, order update or even birthday well wishes.

What can I do to protect myself?

First and easiest thing; slow down and don't rush through your emails etc. We know that is easier said than done when trying to stay caught up on things. But really, simply slowing down and really thinking about the email or online communications you are receiving will go a long way in providing protection.

Ask yourself basic questions before clicking on that link in your email or the attachment that came with it. Example: *Why would you be receiving notification of pending delivery for your order from a store you have never been bought anything from?* A lot of people get so excited they are getting an unexpected package, they do not think before hitting that link in the email to gain delivery status.

Once that link is activated, your machine or device can be loaded with malware or data extraction software, even tracking and keystroke software exposing all your private information, contact list etc.

Please keep in mind, just because nothing appeared to happen after you clicked on that link or attachment, you will probably never realize what has happened. *Most online crooks don't send you a thank you note or screen pop congratulating you on being hacked.*

Additional Actions to Protect:

Hover over any link or email address associated with the emails. You can see the originating source or "spoof" info by simply hovering over those addresses and links. If you do not recognize the source, do not click on anything or open the email and or attachments. An example would be email address says bankofamericasuperx.com, that is probably not an official Bank of America email and should not be trusted.

Verify the "from" address – if you don't know them, do not open.

Implement processes for approval, ask your IT Department or service provider to review anything you have concern about.

Go to the actual web page for the email originator. Example: Netflix sent you an email with a link to reset your password as a result of a breech on their systems. Do not click on the link, rather open another browser session and go to your account with Netflix, look for notification in their messaging system. Or better yet, update your password on their web page.

Always keep a backup of all your data, contacts etc. That way if you do fall prey to the scam, you can have your data restored and hopefully be no worse for wear.

Keep these basic principals in mind:

Do not let habit and familiarity lead to carelessness

If it sounds too good to be true, it probably is, so don't open it.

Be accountable and let someone know if you think you made a mistake, better to have a chance to stop and correct the action.

Change your passwords frequently, consider using a password locker.

Open only if you know!!!

Think about unusual request before acting; *example; your boss sends you an email to go buy $1,000 in gift certificates and send him back an email with all the gift card numbers. SLOW DOWN, maybe send your boss a separate email, NOT RESPONDING to the original and ask them if they really sent you that note? Better yet, call your boss and ask them.*

Interesting facts:

Over 30% of users still base their passwords on birthdays, addresses, pet's name as work passwords. Those are easily replicated

80% of cyber-attacks involve weak or stolen passwords.

More than 1 out of 131 emails contain malware.

95% of all security incidents involve human error

Over 25% of workers let family and friends use company PCs for personal access.

51% connect their own devices or gadgets to their work PC or send work emails to their personal email accounts.

Top examples of Phishing Attack Subject Line or Topics:

- ✓ Restart your membership request
- ✓ Update your Official Record
- ✓ Click to learn more
- ✓ You missed a delivery
- ✓ Confirm your account
- ✓ Your account has been locked
- ✓ Suspended Account
- ✓ Tax Refund
- ✓ Refund due to System Error
- ✓ Click to revise your salary information
- ✓ Sent from your CFO, CEO, President

#1-year end and year out, emails or messaging relating to invoice-based questions/info

Overall, ensure you have some level of network and data security policy for your company/business.

Please let Venture Pointe help you with the creation, testing and implementation of security policies and their enforcement.

Venture Pointe, Inc
8659 Baypine Road, Suite 106
Jacksonville, FL 32256

Phone: (904)351-8101
Fax: (904)301-9081
Email: info@venturepointe.com