UPPER PENINSULA
STATE BANK
You're Going To Like It Here!

Phishing/Spear Phishing

Phishing/Spear Phishing (which has absolutely nothing to do with fishing), is a very common form of fraud still being used today. ***Phishing*** is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, instant message, or other communication channels. ***Spear Phishing*** is an email spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data.

How does it work? The "phisher" falsely claims to be an established legitimate enterprise and uses email to direct the user to visit a website where they are asked to update personal information such as passwords, credit card, social security, and bank account numbers which the real legitimate organization already has. These websites are bogus or fictitious websites, created to look like the real ones, but set up only to steal the user's information. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain or trade secrets and usually appear to come from a trusted source or from someone in a position of authority.

Why does it work or continue to work? This scam uses social engineering - a non-technical intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. The "phisher" will research social media sites and/or corporate website to gather their information in an attempt to make the email appear to be legitimate to the recipient. These phishing campaigns are often build around the current year's major events, holidays and anniversaries or take advantage of breaking news stories, both true and fictitious.

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
WAIT FOR IT
Enter your bank account number.
SCAM.
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Dilbert.com DilbertCartoonist@gmail.com
5-19-14 ©2014 Scott Adams, Inc./Dist. by Universal Uclick

Popular Spear Phishing tactics:

- Thrives on familiarity – the salutation on the email message is likely to be personalized: "Hi Bob" instead of "Dear Sir."
- Email may make reference to a "mutual friend" or a recent online purchase you've made or create a plausible, persuasive premise: account alert, update your information, mandatory password change, etc.; may also include a link to a website used for gather information
- Use of the legitimate company's domain name in the "from" portion of the "BAIT" email: @ebay.com, @paypal.com, @citibank.com

Some advice to avoid becoming the next victim. If you're not a customer of a company that appears to be sending you an email, ignore it. Even if you are a customer, never respond directly to the email with personal or financial information – use the "***Stop-Look-Call***" technique:

Stop: Do not react to phishing ploys consisting of "upsetting" or "exciting" information
Look: Look closely at the claims in the email, and carefully review all links and web addresses
Call: Do not reply to emails requesting you to confirm account information; call or email the company in question to verify if the email is legitimate

NEVER enter a website from an email link. Check your statements - if you notice anything irregular on your bank account contact your bank immediately. Awareness is the key. The more you know and share with others, the less chance you and others have of being caught *"hook, line, and sinker."*

References:

- Rouse, Margaret. "Spear Phishing Definition." *Whatis.com*. Tech Target, Mar. 2011. Web Mar. 2011.
- Rouse, Margaret. "Phishing Definition." *Whatis.com*. Tech Target, Oct. 2015. Web Oct. 2015.
- "Spear Phishing: Scam, Not Sport." *Norton*. Norton. < http://us.norton.com/spear-phishing-scam-not-sport/article >