PREVENT YOURSELF FROM BEING PHISHED

Phishing steals identities and wrecks lives. It affects everyone, from a senior bank manager to a minor who has never heard of internet scams. The worst part is that though phishing is now more than a decade old, many people are not familiar with how it works and still fall victim to this scam.

WHAT IS PHISHING?

- Using data to access a victim's account and withdrawing money or making an online transaction, e.g. buying a product or service.
- Using data to open fake bank accounts or credit cards in the name of the victim and using them to cash out illegal checks, etc.
- Using the victim's computer systems to install viruses and worms and disseminating phishing emails further to their contacts.
- Using data from some systems to gain access to high value organizational data such as banking information, employee credentials, social security numbers, etc.

PHISHING ON THE RISE

This has become a growing threat in the world of today, and in 2016 they hit a 12-year high. Tara Seals' US North America News Reporter, Infoescurity Magazine noted that they Anti-Phishing Working Group documented a 250% increase in phishing sites between October 2015 and March 2016. There has also been a noted that 93% of phishing emails are now ransomware.

TIPS ON STAYING SAFE

Keep Informed About Phishing Techniques - New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one.

Think Before You Click! - A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name.

Install an Anti-Phishing Toolbar - Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it.

Verify a Site's Security - As long as you are on a secure website, however, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar.

Check Your Online Accounts Regularly - If you don't visit an online account for a while, someone could be having a field day with it. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

10 TIPS TO STAY SAFE ONLINE

- **Know the scams.** Read articles and blogs, follow the news, and share this so you can learn about different kinds of scams and what you can do to avoid them and also help your friends.
- **Think before you click.** Never click on links in messages from people you don't know or vaguely know. These phishing emails have links that lead to websites that can lure you into giving personal information or download malware to your computer
- **Safely peruse.** Beware of phony websites. These sites may have an address that's very similar to a legitimate site, but the page can have misspellings, bad grammar or low resolution images.
- **Shop safely.** Don't shop on a site unless it has the "https" and a padlock icon to the left or right of the URL. Also, protect yourself and use a credit card instead of a debit card while shopping online—a credit card company is more likely to reimburse you for fraudulent charges.
- **Creative passwords.** Do away with the "Fitguy1982" password and use an extremely uncrackable one like *9&4yiw2pyqx#*. Phrases are good too. Regularly change passwords and don't use the same passwords for critical accounts. For more tips on how to create strong passwords, go to http://passwordday.org/
- **Protect your info. Keep your guard up.** Back-up all of your data on your computer, smartphone and tablet in the event of loss, theft or a crash. Also, routinely check your various financial statements for questionable activity.
- **Watch your Wi-Fi connectivity.** Protect your network by changing your router's default settings and making sure you have the connection password-protected.
- **Install a firewall.** A firewall is a great line of defense against cyber-attacks. Although most operating systems come with a firewall.
- **Keep up to date.** The best security software updates automatically to protect your computer. Use the manufacturer's latest security patches to make regular updates and make sure that you have the software set to do routine scans
- **Use your noggin.** You do not need to be a seasoned computer whiz to know that it's not smart to open an attachment titled, "Claim Your Inheritance!" Using common sense while surfing the Web can protect you from some hungry cyber-shark.

TIPS TO STAYING SAFE ON SOCIAL NETWORK

Social networking is the *killer app* of the Internet for everyone – not just the texting crowd. Here are a few tips on how to stay safe on social networks.

TIP 1 – Beware of Too Much Information
Protecting yourself from sharing Too Much Information (TMI) can save you from identity theft and even protect your physical safety.

TIP 2 – Customize privacy options
Social networking sites increasingly give users more control over their own privacy settings. Don't assume you have to take whatever default settings the site gives you.

TIP 3 – Limit work history details on LinkedIn
It would be too easy for identity thieves to use the information to fill out a loan application, guess a password security question (like hackers did with VP candidate Sarah Palins' Yahoo account) or social engineer their way into your company's network.

TIP 4 - Don't trust, just verify
Faking an identity has a legit side too – it can be used by people who simply want to conceal who they are in order to protect their real identities.

PHISHING E-MAIL EXAMPLE AND TIPS

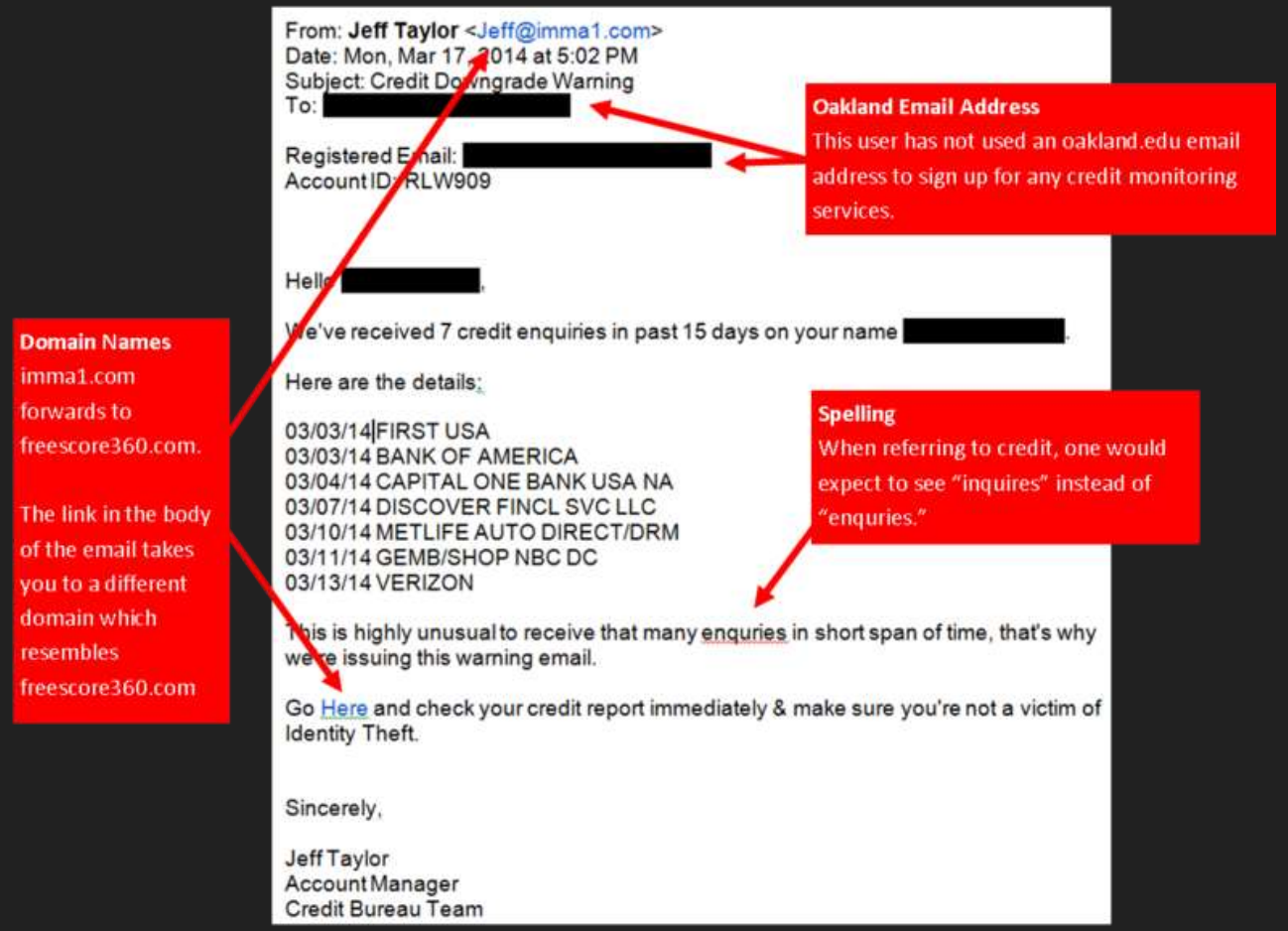
Unfortunately, there is no one single technique that works in every situation, but there are a number of things that you can look for.

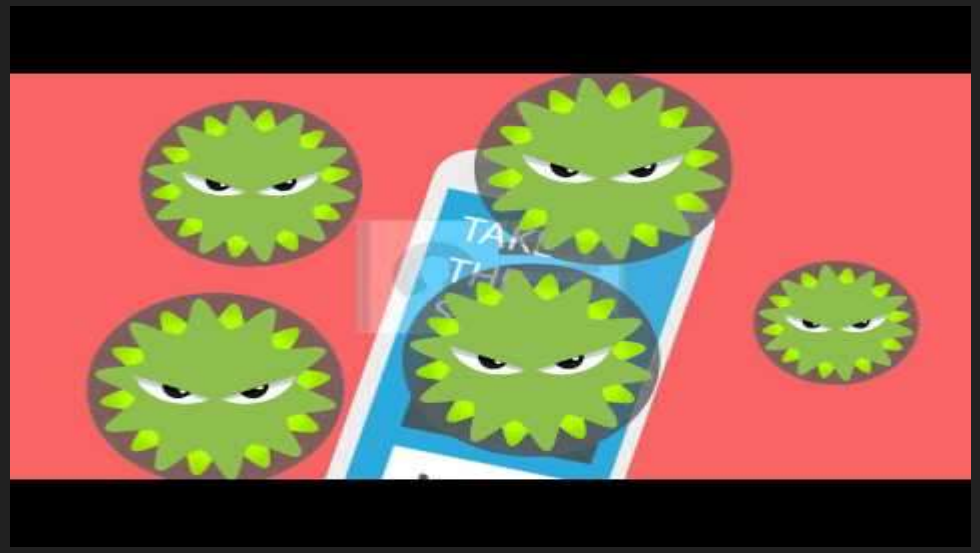
1: The message contains a mismatched URL
Oftentimes the URL in a phishing message will appear to be perfectly valid. However, if you hover your mouse over the top of the URL, you should see the actual hyperlinked address (at least in Outlook).

2: URLs contain a misleading domain name
People who launch phishing scams often depend on their victims not knowing how the DNS naming structure for domains works. The last part of a domain name is the most telling.

3: The message contains poor spelling and grammar
Whenever a large company sends out a message on behalf of the company as a whole, the message is usually reviewed for spelling, grammar, and legality, among other things.

4: The message asks for personal information
No matter how official an email message might look, it's always a bad sign if the message asks for personal information. Your bank doesn't need you to send it your account number. It already knows what that is.





Cybercrime Exposed: How to Spot a Phishing Scam

What is Phishing and How do I Protect Myself

Mythbusting about Mac Computers' Security

Phish Quizzes

https://www.opendns.com/phishing-quiz/

https://www.lookingglasscyber.com/blog/phishing-quiz-whats-your-aptitude/

https://community.spiceworks.com/topic/1175392-quiz-gone-phishing

Thank You