Crossing the Digital Divide (v106)

“Phishfry”
By Joseph Feigon
For the Observer

What is phishing?

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. The word is a neologism\created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. According to the 2013 Microsoft Computing Safety Index, released in February 2014, the annual worldwide impact of phishing could be as high as US$5 billion.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that distribute malware.

Phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in current web security.[8] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Last year, despite all efforts by law enforcement and a multitude of security vendors, incidents of phishing continue to escalate:

- In 2017 76% of organizations experienced phishing attacks. Nearly half of information security professionals surveyed said that the rate of attacks increased from 2016.
- In the first half of 2017 businesses and residents of Qatar were hit with more than 93,570 phishing events in a three-month span.
- A phishing email to Google and Facebook users successfully induced employees into wiring money – to the extent of US$200 million – to overseas bank accounts under the control of a hacker. He has since been arrested by the US Department of Justice.[116]
- In May 2017, the Wannacy ransomware attack is suspected of having impacted more than 230,000 people in 150 countries
- In the beginning of June 2017, a Ukrainian FinTech company, MeDoc, was breached, and its systems were injected with malware called Petya. Through a Microsoft vulnerability, the malware spread across the globe – impacting hundreds of organisations in Russia, Europe, India and the United States.

- By the end of June, a new series of attacks called Not-Petya has wrought havoc globally, shutting down hundreds of businesses, including Maersk, WPP, TNT, Mondelez, Cadburys, Russian steel and oil firms Evraz and Rosneft, Kiev airport and Chernobyls monitoring systems.
- In August 2017, customers of Amazon faced the Amazon Prime Day phishing attack, when hackers are sending out seemingly legitimate deals to customers of Amazon. When Amazon's customers attempted to purchase the 'deals', the transaction would not be completed, prompting the retailer's customers to input data that could be compromised and stolen.

Phishing, in its worst form, is social engineering – creating false images and or fake instances of "trusted" websites in order to separate you from your money. Keep your hands on your wallet, make sure you're using a secure (see the lock in the navigation bar of your browser) website when making purchases, and be sure to keep your computer software up-to-date. If a deal looks too good to be true, run.

Control those things you can, and keep the surprises to a minimum!