



When in Doubt
Throw it Out!

PHISHING: DON'T GET HOOKED BY A SCAM!

Outline

- ▶ Phishing Defined
- ▶ Phishing Terminology
- ▶ How to identify a Phishing attempt
- ▶ How to protect yourself from being Phished
- ▶ Examples
- ▶ Resources available to you if you have been Phished
- ▶ Summary
- ▶ Questions ?

Phishing Defined

- ▶ Phishing : is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by impersonating a trustworthy source, normally by email.
- ▶ Phishing Methods
 - ▶ Spoofed – A fraudulent e-mail sent to mask as a legitimist company
 - ▶ Confirmation Emails – Are one of the most common spoofed emails.
 - ▶ Such as UPS,USPS, FEDEX, or any Retail store.
 - ▶ Helpdesk or Support emails – Are sent to have a user click a link within the email to “fix” an issue with their account.
 - ▶ This is commonly used for accounts that may contain financial or medical information.
 - ▶ Malicious URL –
 - ▶ Malicious URL - <http://www.american.expres.com>
 - ▶ Legitimate URL - <http://www.americanexpress.com>
 - ▶ Use caution when clicking on embedded links as your eyes can play tricks on you as it is easy to miss the subtle differences
 - ▶ Fraudsters are counting on users to miss these minor differences

Phishing Terminology

- ▶ Phishing
- ▶ Spoofed
- ▶ Ransomware
- ▶ Malware
- ▶ Keylogger
- ▶ URL
- ▶ Redirect
- ▶ Marcros & Ad Ons

Identify Phishing Attempt

- Are you expecting files to large to email?

From: Frank D. Samperi, Esq. [<mailto:fdsamperiesq@aol.com>]

Do we know the sender?

Sent: Saturday, March 22, 2014 11:33 AM

Subject: View This Shared Docs

Hello

I've shared a Google Docs with you at Google Drive

Are you expecting google docs?

To open this document, go to

[CLICK TO VIEW HERE](#)

and sign in with your email to see.

Hover mouse

It's very important.

Thanks.

<http://preetikaguptadds.net/directory/googledocs/index.htm>
mCtrl + Click to follow link

Frank D. Samperi

Attorney at Law

45 Essex Street

Hackensack, NJ 07601

Do we know the sender?

Identify Phishing Attempt

- A closer look
 - At first glance what do we see...

The image shows a screenshot of a phishing email designed to look like a Walmart order confirmation. The email header features the Walmart logo and the slogan "Save money. Live better." Below this is a navigation bar with categories: Electronics, Movies, Home, Baby, Toys, Video games, Photo, and Beauty. The main body of the email contains the following text:

This letter is to advise you about the order we k
You have 4 days to pick it in any Local Store of Walmart.

Please, follow this [link](#) for more inform

Walmart is wishing you Happy Thanksgiving Day!

At the bottom, there is another navigation bar with links: Store Finder, Local AD, Returns & Exenches, Privacy & Security, and Help. The footer contains the text: "Copyright (c) 2014 WalMart | All rights reserved".

Three red arrows point to specific elements in the email:

- An arrow points to the Walmart logo with the text: "Do you know the sender?"
- An arrow points to the main body text with the text: "Do you normally purchase confirmations?"
- An arrow points to the "link" text with the text: "Hover the Mouse?"

Link: <http://celikerfiberglass.com/title.php?dp=MTrtmPxGkh3ItCTirf9LY4Ezg+kLNqRUZI9bMYTN3hA=>

A user who received this email...



The screenshot shows a ransomware message window titled "CryptoLocker". The background is red. On the left, there is a blue shield icon with a white cross. Below the shield, the text reads: "Private key will be destroyed on 3/2/2014 10:39 AM" and "Time left 46 : 55 : 55". On the right, a white box contains the following text: "Your personal files are encrypted! Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this. Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt the files you need to obtain the **private key**. The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files... **To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **400 USD / 400 EUR / similar amount in another currency**. Click «Next» to select the method of payment. **Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**" At the bottom right, there is a blue button labeled "Next >>".

.... Opened the Attachment ☹

Top Ten 10 Phishing Attempts 2014

▶ Phishing Scams of 2014

- ▶ 10. Fax Notice
- ▶ 09. Bank Alert, installs Keylogger
- ▶ 08. Message from Attorney
- ▶ 07. Email delivery failure installs Ransomware Phishing
- ▶ 06. Payroll, ADP, with PDF (malware) attachment.
- ▶ 05. IRS, tax collection.
- ▶ 04. Fax notice, with banking malware.
- ▶ 03. .EDU domain that offers remote access.
- ▶ 02. Dropbox, offers malware or crypto-malware instead.
- ▶ 01. Unknown sender or 3rd party file share, offers malware & remote access.

Summary

- ▶ Phishing. It's old school but it still works.
- ▶ Think before you click!
- ▶ Privacy is everyone's responsibility
- ▶ Just like your personal data, your employer needs to ensure its privacy too.
- ▶ A targeted phishing mail was sent to a number of celebrities, enticing them to enter their iCloud credentials onto a fake login page would do the job just as well as any more complex hack.
- ▶ Do not open attachments or click links in unusual email, text, or instant messages (IM), on social networks, or in random pop-up windows.

- ▶ Questions to ask yourself:
 - ▶ Do you know the sender?
 - ▶ Does the attachments make sense (do you normally receive invoices as
 - ▶ Be extremely cautious if you receive an email, text messages, or messages from social networks like Facebook, LinkedIn, and Twitter.
 - ▶ You should you be suspicious of links and attachments from someone on your team?