Not Too Much: When to Share

Strategic Partnership Program
FBI Washington Field Office
Strategic Partnership Program

- National outreach effort to Cleared Defense Contractors (CDC’s), Academic institutions, think tanks
- Mutually beneficial relationships
- Provide CI training to personnel
- If requested, assist in developing internal counterintelligence programs

PROTECTION is the goal
You and counterintelligence protect our most valuable assets, which include our:

- People
- Facilities
- Sensitive information
- Technology
• What have been your experiences?
What is Phishing?

• Attempting to acquire information by masquerading as a trustworthy entity
• Directs user to enter details on a fake website whose look and feel are almost identical to legitimate one
Characteristics of Phishing

• False identity provided by criminal
• E-mail spoofing (fake e-mail)
• Often looks legitimate
• Requests information
• Sent in bulk
Characteristics of Phishing

- Trustworthy entity
  - Popular social websites
  - Auction sites
  - Online payment processors
  - IT administrators

- Types of information Requested
  - Usernames
  - Passwords
  - Credit card details
• Attackers spoof the Address bar
  – Can I make the real Address bar disappear?
• Attackers spoof the lock
  – Not good… we’ve trained users to look for https:// and the lock
Common Attack Methods

- Websites
  - Fake websites
  - Fake pop-ups
  - Fake websites with validation

- Social Networks
  - Facebook
  - The friend search
  - Twitter
A domain name similar to a legitimate site is bought and molded to look exactly like the real thing. The phisher then sends out messages, either by e-mail, instant messaging, Facebook messages, text messages, and so forth to fool a victim into clicking a link to the fake site. The unsuspecting victim logs in and their credentials logged.
Fake Website: PayPal Login?

Member Log In

Registered users log in here. Be sure to protect your password.

Email Address: 
Password: 
Forget your password?

New users sign up here! It only takes a minute.

The Fast, Safe, Easy Way to Pay

PayPal is a global leader in online payments. Find out more.
Fake Pop Up

• An evolution of the 'Fake Website' attack
• Instead of linking to a fake website, there is a link to the actual website
• When the actual website loads, a pop-up appears asking for the user's credentials
• The victim, seeing the legitimate site in the background thinks the pop-up is from a legitimate source and enters their information
Another evolution of the 'Fake Website' attack was to have the fake website verify the victim's credentials with the real site.

A victim would enter their credentials, the fake website would send the credentials to the real website and automatically validate whether the username and password is correct or not.

Saving the hacker's time by having auto validation.
The allowance of applications and a new internal messaging system

A victim could be surfing on Facebook when they receive a message from someone linking to a site.

The victim clicks the link and lands on a login page that looks exactly like Facebook's login page.

The victim enters their credentials.
• The allowance of applications and a new internal messaging system
• A victim could be surfing on Facebook when they receive a message from someone linking to a site
• The victim clicks the link and lands on a login page that looks exactly like Facebook's login page.
• The victim enters their credentials
Social Networks- Twitter

• Hackers use Twitter and tweet links to a fake version of the Twitter site
• They use methods to shorten the real URL
• On their tweet, they put a shortened link with a comment to have curious victims click the link
• When the victim clicks the link a fake Twitter site loads
• The victim puts in their credentials and gives away their password
Method of Delivery: E-mail Spoofing

From: Paypal.co.uk [Alerts@paypal.co.uk]  
To: Eliza Mills  
Subject: Paypal Account Notification.

Dec 2009

Dear users of PayPal services,

Due to upcoming changes in our Service Agreement in December 2009, you will need to submit additional details on your PayPal account. Starting in 2010 all PayPal accounts will come with complete detailed information! Identity protection matters. And PayPal works day and night to help keep your identity safe.

Identity protection matters. Get Verified!

According to the new changes in our Service Agreement, any unverified account will be deleted from the system in 72 hours after receiving this notice.

<table>
<thead>
<tr>
<th>Your Account</th>
<th>Identity Protection Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tips to Protect Your Account</td>
<td>New spoof tutorial</td>
</tr>
<tr>
<td>Paypal's world class fraud investigators share 5 important</td>
<td>Learn how to spot and avoid fraudulent &quot;spoof&quot; emails and websites with PayPal's handy 5-step spoof tutorial.</td>
</tr>
</tbody>
</table>

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
How Phishing Works

A hacker sends a fake or "spoofed" email that appears to be from a trusted company.

The email usually instructs the user to login to verify information, and contains a link.

The link in the email directs the user's web browser to a fake website operated by the hacker.

The fake website looks exactly like a company's real website, and requires the user to login.

Any information the user enters into the fake website is immediately delivered to the hacker, which they can use to access the user's accounts.
Email messages designed to convince unsuspecting victims:

- To take an action
  - Click on link and provide information
- That a threat is associated with non-action
  - Close bank account / credit card
  - Close Ebay account
  - Vulnerable to security risk
Email messages designed to convince unsuspecting victims:

- To take an action
  - Click on link and provide information
- That a threat is associated with non-action
  - Close bank account / credit card
  - Close Ebay account
  - Vulnerable to security risk
Organizations and Countries target Americans:

- Foreign Intelligence services
- Terrorist organizations
- Criminal organizations
- Foreign companies
Information that is valuable and targeted includes:

- **Classified** and **Unclassified**
- Trade secrets
- Financial and regulatory information
- R&D
- IT systems
- supply chain
Why would they target you?

Organizations and Countries target Americans:

- Foreign Intelligence services
- Terrorist organizations
- Criminal organizations
- Foreign companies
Why you might be targeted

Access (What you know)

Influence (Who you know)
Intelligence collectors target Americans using many legal and illegal techniques

Overt collection
- Elicitation
- Open source
- Negotiating & Bidding

Technical collection
- Cyber
- Signals

Covert collection
- Recruitment (Insider Threat)
Universities Vulnerable?

Report in March of 2014:

- Phishing scheme targeted graduate students
- Obtain sensitive personal information
- Method: receive private tutoring for dependant
- One victim deposited check, wire out $
Anti-Phishing Working Group 2\textsuperscript{nd} Quarter 2014:

- 128,378 phishing sites observed
- Payment services most targeted sector
- Crypto-currency sites targeted more
- U.S. is top country hosting phishing sites
- 15 million new malware samples gathered
Avoid the Scam

-Don’t click on link to confirm, contact company
-Avoid e-mailing personal and financial information
-Review credit card and bank account often
Internet Crime Complaint Center:

www.IC3.gov
The IC3 has taken the lead in forging necessary partnerships among the FBI, state and local law enforcement agencies to fight internet crime.

- The IC3 is the central component of the FBI’s plans to develop a national platform to comprehensively address the global threat of internet crime.
- Leverages the intelligence contained in victim reports submitted to the IC3 with the investigative resources of the FBI’s Cyber Task Forces consisting of FBI Special Agents and cyber-trained investigators from state and local law enforcement agencies around the country.
- The IC3 uses its complaint database and analytical capabilities to create targeted intelligence packages that are connected to a particular jurisdiction.
- The targeted packages are sent to the Cyber Task Force in an FBI field office, which includes personnel from the FBI and state and local agencies who are dedicated to investigating and prosecuting internet crime.
Questions?

SA Kescha Wilson
Kescha.Wilson@ic.fbi.gov

FBI Washington Field Office
WFOStrategicPartnership@ic.fbi.gov
202 278-2000