Phishing and Espionage

Jason Hong
Carnegie Mellon University

Human-Computer Interaction Institute
Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your account without warning if we believe that you have violated our User Agreement.
This entire process known as phishing
How Bad Is Phishing?

Consumer Perspective

- Estimated ~0.5% of Internet users per year fall for phishing attacks
- Conservative $1B+ direct losses a year to consumers
  - Bank accounts, credit card fraud
  - Doesn’t include time wasted on recovery of funds, restoring computers, emotional uncertainty
- Growth rate of phishing
  - 30k+ reported unique emails / month
  - 45k+ reported unique sites / month
How Bad Is Phishing?
Perspective of Corporations

- Direct damage
  - Loss of sensitive customer data

Salesforce.com Warns Customers of Phishing Scam

Salesforce.com is warning customers that they may be the targets of malicious software or phishing scams, after one of its employees was tricked into divulging a corporate password.
How Bad Is Phishing?

Perspective of Corporations

- Direct damage
  - Loss of sensitive customer data
  - Loss of intellectual property

Spear-Phishing Attacks Out Of China Targeted Source Code, Intellectual Property

Attackers used intelligence, custom malware to access Google, Adobe, and other U.S. companies' systems
How Bad Is Phishing?

Perspective of Corporations

• Direct damage
  – Loss of sensitive customer data
  – Loss of intellectual property
  – Fraud
  – Disruption of network services

• Indirect damage
  – Damage to reputation, lost sales, etc
  – Response costs (call centers, recovery)
    • One bank estimated it cost them $1M per phishing attack
Phishing Increasing in Sophistication

Targeting Your Organization

- **Spear-phishing** targets specific groups or individuals

- Type #1 – Uses info about your organization

Indira Nair is retiring next week, [click here](#) to say whether you can attend her retirement party
Phishing Increasing in Sophistication

Targeting Your Organization

- Around 40% of people in our experiments at CMU would fall for emails like this (control condition)
Phishing Increasing in Sophistication

Targeting You Specifically

- Type #2 – Uses info specifically about you
  - Social phishing
    - Uses information from social networking sites
    - Ex. Fake email from friends
    - Ex. Fake email from co-worker
  - Fake videos of you and your friends
    - Uses publicly available information
    - Used to install malware or get passwords
Phishing Increasing in Sophistication
Targeting You Specifically

Here’s a video I took of your poster presentation.
Phishing Increasing in Sophistication
Targeting You Specifically

• Type #2 – Uses info specifically about you
  – Whaling – focusing on big targets

Thousands of high-ranking executives across the country have been receiving e-mail messages this week that appear to be official subpoenas from the United States District Court in San Diego. Each message includes the executive’s name, company and phone number, and commands the recipient to appear before a grand jury in a civil case.

-- New York Times Apr16 2008
Phishing Increasing in Sophistication
Combination with Malware

- Malware and phishing becoming combined
  - Poisoned attachments (Ex. custom PDF exploits)
  - Links to web sites with malware (web browser exploits)
  - Can install keyloggers or remote access software

Spear-Phishing Attacks Out Of China Targeted Source Code, Intellectual Property

Attacks used intelligence, custom malware to access Google, Adobe, and other U.S. companies' systems

Jan 13, 2010 | 04:12 PM

By Kelly Jackson Higgins
DarkReading

The wave of targeted attacks from China on Google, Adobe, and more than 20 other U.S. companies, which has led the search giant to consider closing its doors in China and no longer censor search results there, began with end users at the victim organizations getting duped by convincing spear-phishing messages with poisoned attachments.
Sir,

This morning (28 Aug) we received the 211 page India Multi-Role Combat Aircraft (MRCA) Request for Proposal (RFP). The major RFP points are:

- 126 aircraft (86 single seat/40 dual); 18 built by OEM, 108 co-produced in India
- 1 or 2 engines; 14k-30k kg (30.9k-66.1k lb) max weight
- Active AESA radar capable of targeting 5 m² at 130km (80.8 miles)
- 24 month fixed price validity of offer; option for 63 aircraft good for 3 years (fixed price)
- 50% Offset requirement
- Aircraft delivery to begin 36 months from contract, co-production begins 48 months from contract
- Tech transfer is broken into 5 categories, 60% is the highest percentage
Who is Doing These Attacks?

- Not many documented phishing attacks for corporate espionage (yet)
  - Not many have been caught or willing to admit being victim

- Actors
  - Government-backed groups (not just China!)
  - Cybercriminals looking for more fertile grounds
  - Corporate rivals

- Victims
  - High-tech organizations (intellectual property)
  - Defense contractors
What Can We Do About Phishing?

• Better mail filters / malware detectors
• Better indicators of what sites we are going to
• More automated software updates
• Better training and awareness
  – People are an integral part of computer security, but are also the most often overlooked component
Summary

- Phishing is a plague on the Internet
- Phishing is increasing in sophistication
- Starting to see early forms of espionage, only going to get worse
PhishGuru Embedded Training

• A lot of training materials are boring and/or ignored
• Can we “train” people during their normal use of email to avoid phishing attacks?
  – Periodically, people get sent a training email by admins
  – Training email looks same as a phishing attack
  – If person falls for it, intervention warns and highlights what cues to look for in succinct and engaging format
Subject: eBay: Urgent Notification From Billing Department

From: eBay Inc <identdep_op107@ebay.com>
Date: 8/6/2005 10:26 PM
To: jasonh@EECS.Berkeley.EDU

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn.sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your account if you violate our rules or guidelines, without notice or liability.

Thank you for being a valued customer. If you have any questions, please contact us at support@ebay.com.
Everyday Privacy and Security Problem

Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams

The victim

This email is from my bank and it is asking me to update my information. I better click on the link and update it.

STOP!
Don't fall for this scam email.

The phisher

Here's how con artists try to steal your personal information.

ABC BANK
From: service@ABCBank.com
To: Jane@myemail.com
Dear Jane,
Your account will be suspended if you do not update your information,
http://www.ABCBank.com/update

I forged the address to look genuine.
I threatened the user with an urgent message.
I added a link that looks like it goes to ABC Bank – but it really sends people to my site so I can steal their information and money!

ABC BANK
From: service@ABCBank.com
To: Jane@myemail.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.ABCBank.com/update

Thanks PhishGuru! Where should I report suspicious emails?
Send them to reportphishing@antiphishing.org

WARNING!
The web page you tried to visit was reported to be a phishing scam. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

1. Don't trust links in an email.
http://www.ABCBank.com/update

2. Never give out personal information upon email request.
Name: Jane Smith
SSN: 123-45-6789

3. Look carefully at the web address.
http://www.amazon.com

4. Type in the real website address into a web browser.
http://www.ANNAn.com

5. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
For customer service call 1-800-xxx-xxxx

6. Don't open unexpected email attachments or instant message download links.
My Inbox
Here is the updated document.
attachment

To learn more about protecting yourself from phishing scams visit http://phishguru.org
Learning science principles
- Learning by Doing
- Immediate feedback
- Conceptual-Procedural Knowledge
Phishing Becoming Pervasive

Social Media

Beware the new Facebook password reset scam

Twitter Phishing Attack Hooks UK Cabinet Minister

The company is warning people not to surrender personal details to fake Twitter login pages.

By Thomas Claburn
InformationWeek
February 26, 2010 01:21 PM

A phishing attack on Twitter has claimed several high-profile victims including a British cabinet minister and a bank.

Ed Miliband, the U.K's Secretary for Energy and Climate Change, on Friday found his Twitter account sending
Phishing Becoming Pervasive

Current Events

- Disasters
- Sports
- Celebrities
Phishing Becoming Pervasive
Government Services

IRS Warns of Tax Refund Phishing Emails, Other Scams

March 16, 2010 by Staff
Filed under Consumer & Credit Trends

As the tax deadline approaches, the Internal Revenue Service today reminded taxpayers of the most common scams at this time of year, including phishing emails looking for personal

Fraudulent Activity and Scams

The Census Bureau uses a workforce of trained federal employees to conduct a variety of household and business surveys by telephone, in-person interviews, through the mail, and in limited cases through the Internet. We understand your personal information is sensitive, and go to great lengths to protect the data we collect. Although we cannot stop or warn against all bogus or false collections of data -- here are some tips to help you recognize fraudulent activity or unofficial data collections.

If you are contacted for any of the following reasons -- Do Not Participate. It is NOT the U.S. Census Bureau.