



Phishing

Table of contents

1. About phishing
2. Types of phishing attacks
3. How to recognize phishing e-mail scams?
4. What techniques phishers are using?
5. How to protect yourself from phishers attack?
6. Statistics

1. About phishing

Definition of phishing

Phishing is a specific form of cyber crime. Phishing tricks computer users into disclosing personal details such as usernames, passwords, PIN numbers, credit card numbers etc, which are linked to bank accounts or on-line shopping accounts. These details are then used to steal money.

Phishing fraudsters steal your
personal information and then your
money...

History

- The word “phishing” originally comes from the analogy that early Internet criminals used email lures to “phish” for passwords and financial data from a sea of Internet users
- The term was coined in the 1996, timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords

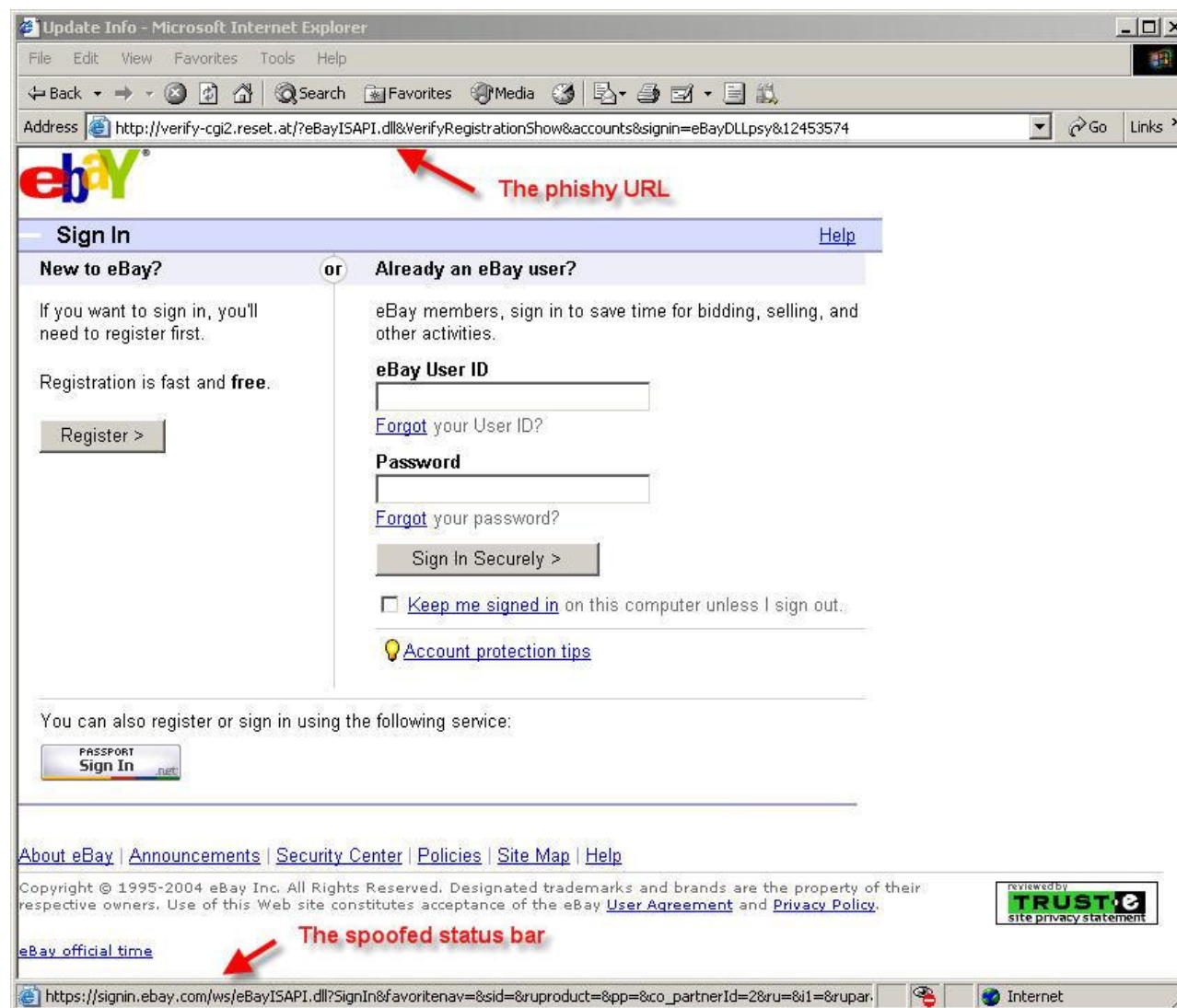
How phishers do it? (1)

- Trick user by replying to e-mail for passwords and credit card details;



How phishers do it? (2)

- Fake websites;



How phishers do it? (3)

- Man-in-the-middle data proxies – delivered through any electronic communication channel



How phishers do it? (4)

- Installation of Trojan horse key-loggers and screen captures;



2. Types of phishing attacks

Phishing attack

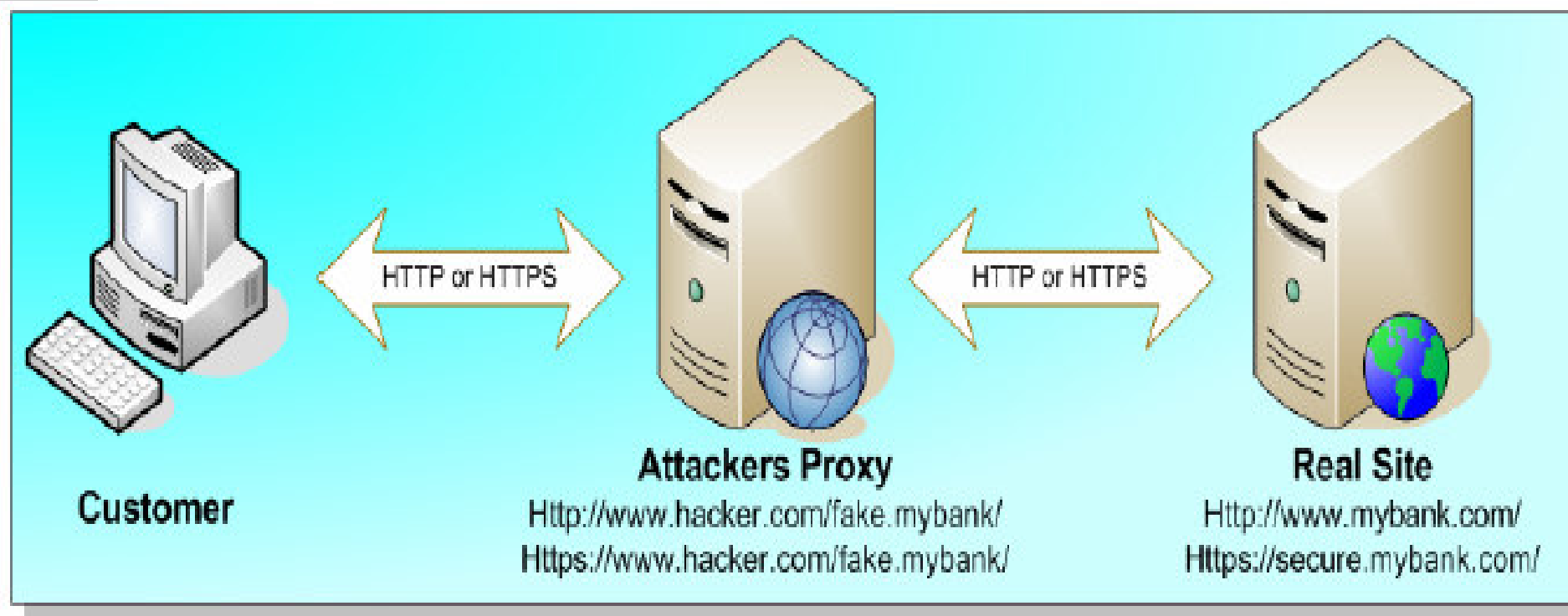
The most common methods for phishing attack are:

- Man-in-the-middle attacks;
- URL obfuscation attacks;
- Preset session attacks;
- Client-side vulnerability exploitation

1. Man-in-the-middle attacks

- The attackers situate themselves between the customer and the real web-based application;
- From this vantage point, the attackers can observe and record all transactions;
- The customer connects to the attackers' server as it was the real site, while the attackers' server makes a simultaneous connection to the real web-based application server – typically in real-time;

1. Man-in-the-middle attack



Update Info - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back

Forward

Stop

Home

Search


Media

Print

Links

Address

http://verify-cgi2.reset.at/?eBayISAPI.dll&VerifyRegistrationShow&accounts&signin=eBayDLLpsy&12453574



Sign In

or

Already an eBay user?

Help

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

Register >

eBay User ID

Forgot your User ID?

Password

Forgot your password?

Sign In Securely >

☐ Keep me signed in on this computer unless I sign out.

Account protection tips

You can also register or sign in using the following service:


PASSPORT

Sign In

About eBay | Announcements | Security Center | Policies | Site Map | Help

Copyright © 1995-2004 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

eBay official time



https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&favoritenav=8&sid=8&rproduct=8&pp=8&co_partnerId=28&ru=&l=8&rupar.

Internet

The phishy URL

The spoofed status bar

1.1. When you are logging in.. (1)

- The phish site will pass the entered information to the legitimate site and will attempt a login;
- If the login fails, e-Bay will return an error, and the phish site will display an error message;

1.2. When you are logging in.. (2)

- If the login succeeds, the phish site will save information and will redirect browser window to the eBay account opened;
- This procedure creates an imitation of an eBay login, but the username and password are intercepted by the scammers

2. URL obfuscation attacks

- The secret for many phishing attacks is to get the message recipient to follow hyperlink (URL) to the attacker's server, without realizing that they have been duped.
- The most common methods of URL obfuscation include:
 - Bad domain names;
 - Third-party shortened URL's;
 - Host name obfuscation;

2.1. Bad domain names

- Web-page for bank is: www.mybank.com
- Financial institute for transactions is:
<http://banking.mybank.com>;
- Possible fraudulent domain names:
 - <http://mybank.banking.com>;
 - <http://mybanking.bank.com>;
 - <http://bank.mybanking.com>;
 - <http://banking.mybonk.com>;
- Be carefull with upper-case “i” and lower-case “L”.

2.2. Third party shortened URL's (1)

Dear valued MyBank customer,

Our automated security systems have indicated that access to your online account was temporarily blocked on Friday 13th April between 02:16 and 02:29 due to repeat 2654 login failures. It is most probable that your account was subjected to malicious attack through automated brute forcing techniques.

While MyBank were able to successfully block attack of your account, we would recommend that you ensure that your password is sufficiently complex to prevent future attacks. To log in and change your password, please click on the following URL:

<https://privatebanking.mybank.com/privatebanking/ebankver2/secure/customersupport.aspx?messageID=1542556&Sess=asp04&passwordvalidate=true&changepassword=true>

If this URL doesn't work, please use the following alternative link which will redirect to the full page – <http://tinyurl.com/5wl2>

Best regards,
MyBank Customer Support

2.2. Third-party shortened URL's (2)

- www.tinyurl.com is one of the engines for making URL smaller;
- The link in mail will not work because it do not exist but the shortened part will contain the malicious code;
- Phishers can use this tool to trick the users;

2.3. Host name obfuscation (1)

- For navigation on Internet a fully qualified domain name such as www.evilsite.com are used;
- For a web browser to communicate over the Internet, this address must to be resolved to an IP address, such as 195.50.20.72 for www.evilsite.com

2.3. Host name obfuscation (2)

- A phisher may wish to use the IP address as a part of URL to obfuscate the host and possibly bypass content filtering systems, or hide the destination from the end user;

- For example the following URL:

<http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm>

could be obfuscated such as:

<http://mybank.com:ebanking@195.50.20.72/login.htm>

What is session?

- Web-based applications must use custom methods of tracking users through its pages and also manage access to resources that require authentication;
- The most common way of managing state within such an application is through Session Identifiers (SessionID's)

3. Preset session attack (1)

- The phishing message contains a web link to the REAL application server, but also contains a predefined SessionID field;
- The attackers system constantly polls the application server for a restricted page using the preset SessionID;
- The phishing attackers must wait until a message recipient follows the link and authenticates themselves using SessionID;

3. Preset session attack (2)

- Once authenticated, the application server will allow any connection using the SessionID to access restricted content;
- Therefore, the attacker can use the preset SessionID to access a restricted page and carry out his attack;

4. Client-side vulnerabilities (1)

- The more functionality built into the browser, the more likely there exists vulnerability that could be exploited by an attacker;
- Unlike worms and viruses, many of the attacks cannot be stopped by anti-virus software as they are much more harder to detect and consequently to prevent

4. Client-side vulnerabilities (2)

- Although software vendors are releasing software updates, home users are not notoriously poor in applying them;
- This, combined with the ability to install add-ons means there are many opportunities for attack;

3. How to recognize phishing e-mail scam?

How the phishing e-mail looks?

- Like a legitimate e-mail from some organization, such as a bank, and contains a link to a webpage;
- Webpage looks identical to the real webpage but it is controlled by the attacker;
- On this page user is prompted to log in;

How to recognize e-mail from an e-tailer, bank or your IT department (1)

- Included a telephone number;
- The grammar and punctuation will be proofed and correct;
- The department that claims to author the e-mail will exist;

How to recognize e-mail from an e-tailer, bank or your IT department (2)

- A return email address will be provided;
- If they ask you to take an action like change a password, they are less likely to give you a hyperlink to click-through.

From: service@paypal.com
Subject: Your PayPal Account



Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

[Click here to verify your account](#)

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, [log in](#) to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

PayPal Email ID PP697

Fraudulent email from PayPal

- Make sure you never provide your password to fraudulent persons
- PayPal will never ask you to enter your password in email
- You should never give your PayPal password to anyone including PayPal employees

How can you recognize phishing e-mail?

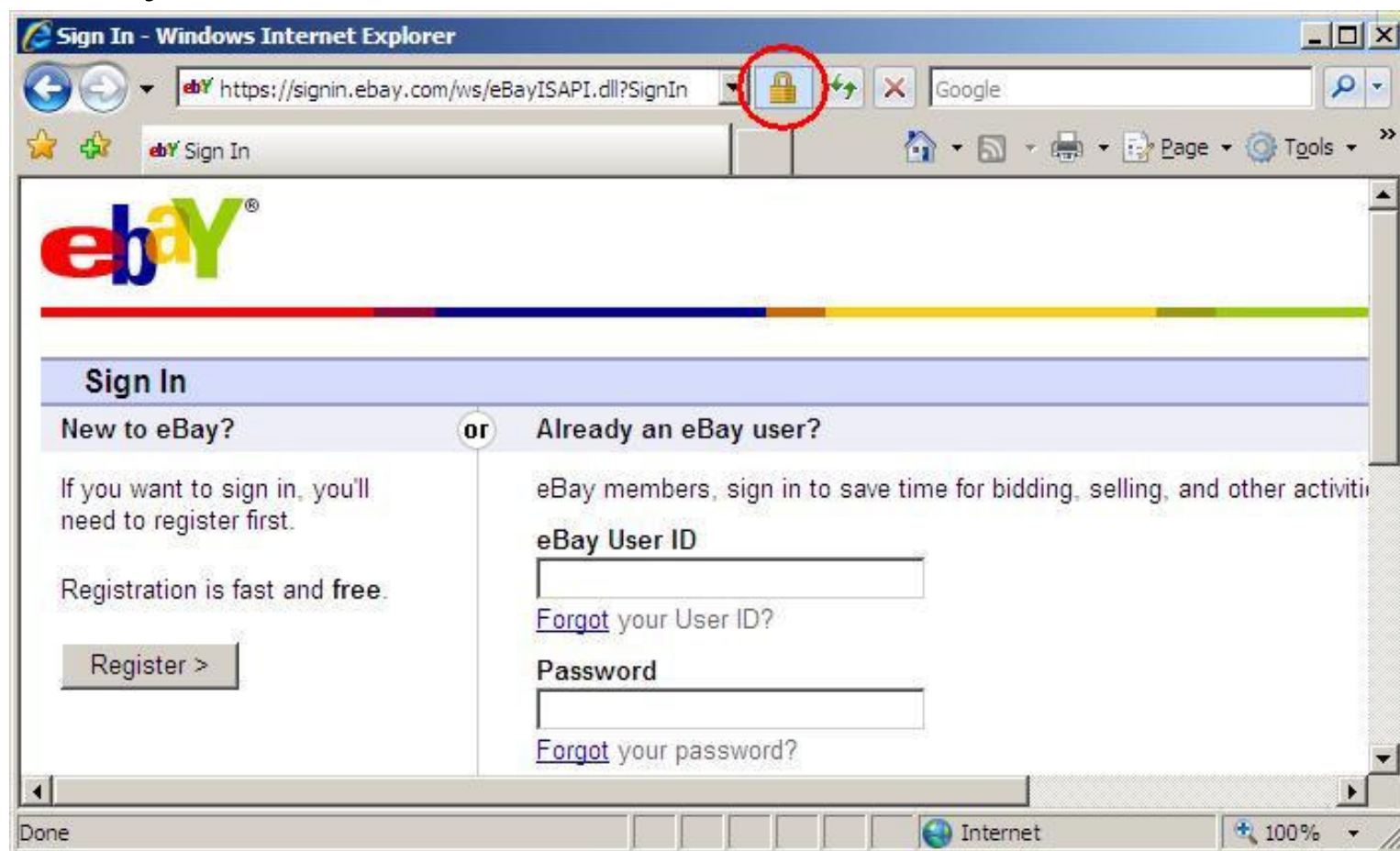
[Click here to verify your account](#)

Actual link URL: http://80.179.238.73/ ... paypal/

- The mail is not addressed particularly for you. The address is “Dear customer” instead;
- In contents is provided a link;
- It says that you have to login as soon as possible in your account for some reason;

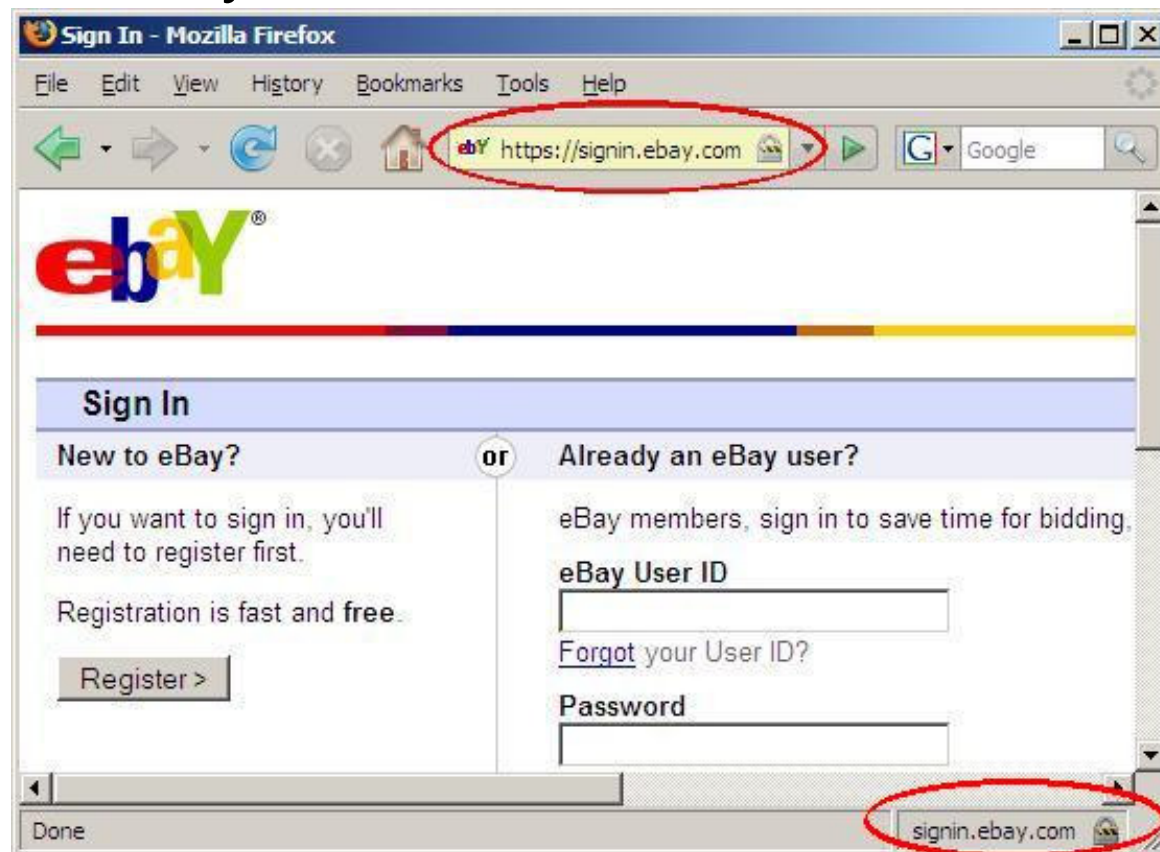
How to recognize secure webpage? (1)

- If you are using Internet Explorer, next to the address bar you can see a lock;



How to recognize secure webpage? (2)

- If you are using Mozilla Firefox, the lock is provided into the status bar and the background of address bar turns to yellow;



4. What techniques phishers are using?

Fake banners

- Very simple method phishers may use;
- Phisher copies a banner;
- Place it on popular web-sites;
- Banner redirects user to the phishing web-site;
- Phisher collects your personal data;

e-mail (1)

- Pretends to be from a well-known company, such as eBay or PayPal or a bank;
- There are used generic greetings.
 - Many spoof e-mails begins with a generic greeting such as: “Dear Bank customer.”

e-mail (2)

- A false sense of urgency.
 - Most spoof emails try to deceive you with the threat that your account is in jeopardy if you do not update it as soon as possible
- Fake links.
 - The text in a link may attempt to look valid, then send you to a spoof address.

IRC and Instant Messaging

- These forums are likely to become a popular phishing ground;
- Phisher anonymously send semi-relevant links and fake information to would-be victims.

Usage of hidden frames (1)

- Hiding the source address of the attacker's content server;
- Used to provide a fake secure HTTPS wrapper for the sites content;
- Hiding HTML code from customer;

Usage of hidden frames (2)

- Loading images and HTML content in the background for later use by a malicious application;
- Storing and implementing background code operations that will report back to attacker what the customer does.

5. How to protect yourself against phishers?

Possible phishing scam

Subject: New virus discovered!

Message body:

A new virus has been discovered! It's name is "Datore". Full list of virus abilities is included in attached file "info.txt". For the last information go to McAfee's web page. Please forward this message to everyone you care about.

Attached file: info.txt.vbs

Legitimate company will never ask you to give:

- Credit and debit card numbers;
- Bank account numbers;
- Driver's license numbers;
- Email addresses;
- Passwords;
- Your full name;

Ways to fight spoof

- Report it
 - Forward the entire e-mail – including the header information – or the site's URL.
- Use SafetyBar
 - There are engineered toolbars for Microsoft Outlook you can use to report spoof emails

Steps to take to prevent spoof from affecting you (1)

- Keep your security current
 - Update your firewalls and security patches frequently;

- Monitor your account
 - Check your account periodically to see if there is any suspicious activity;

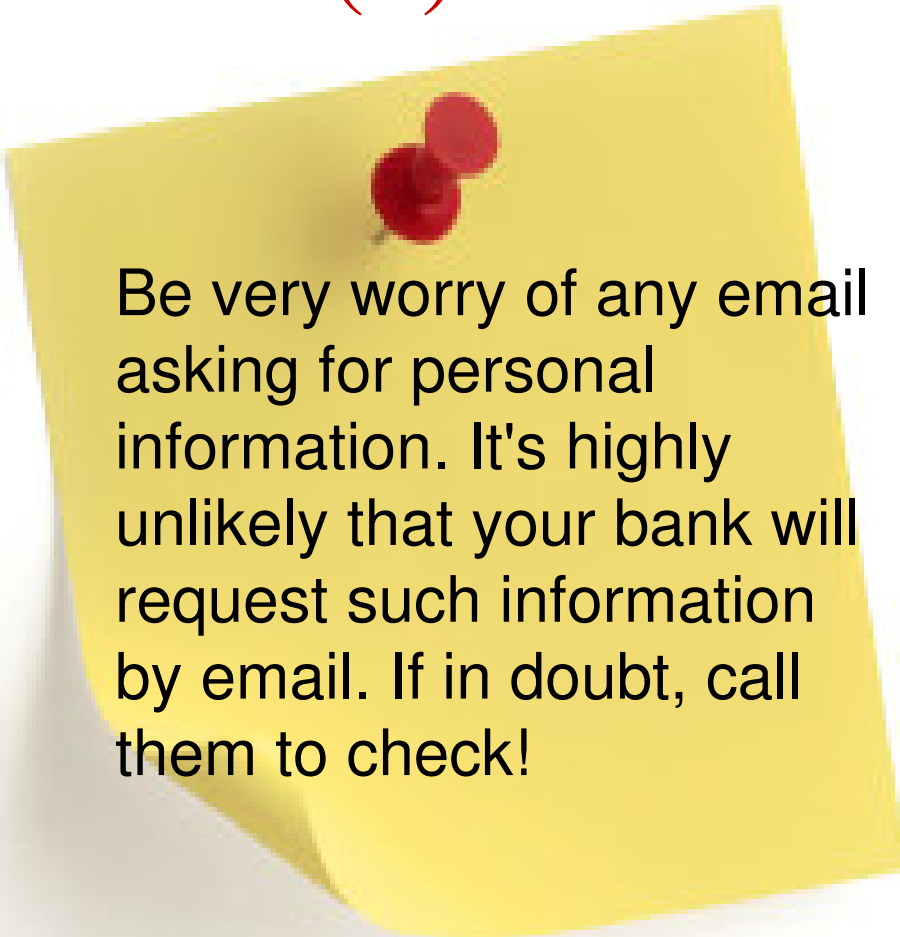
Steps to take to prevent spoof from affecting you (2)

- Change your password often
 - If you think your security may have been breached, create a new password immediately;
- Take action
 - If your information is compromised, get a fraud alert placed on your credit report;

Steps to take to prevent spoof from affecting you (3)


- Use a unique password
 - Your bank account password should be one-of-a-kind, and not used on any of your other accounts. A good password contains letters and numbers.

Tips to follow (1)



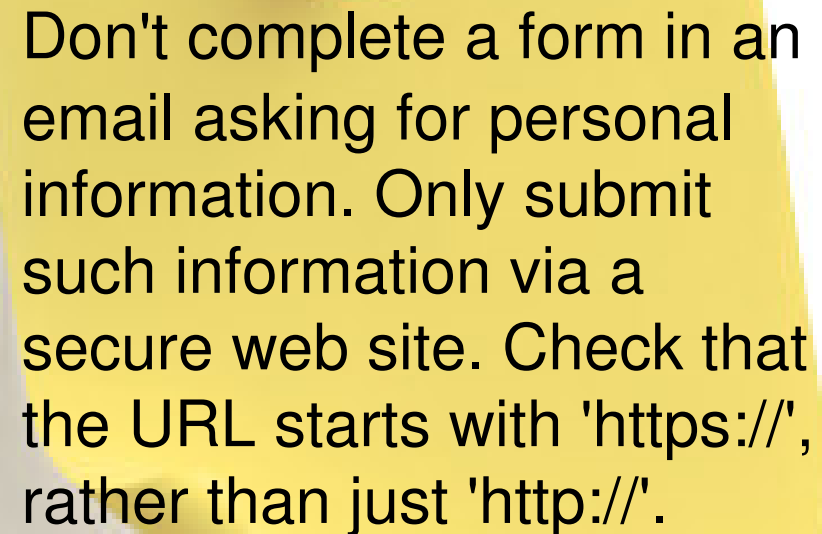
Be very worry of any email asking for personal information. It's highly unlikely that your bank will request such information by email. If in doubt, call them to check!

Tips to follow (2)



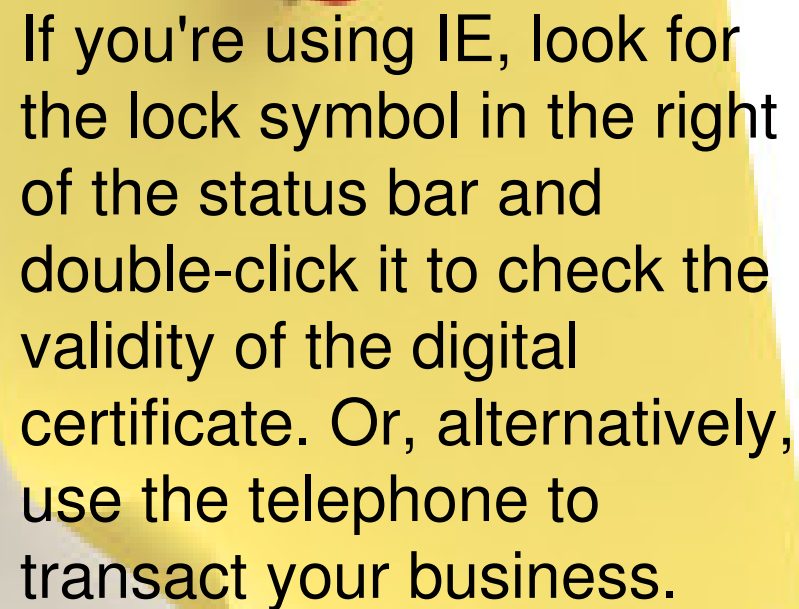
Don't use links in an e-mail message to load a web page. Instead, type the URL into your web browser.

Tips to follow (3)




Don't complete a form in an email asking for personal information. Only submit such information via a secure web site. Check that the URL starts with 'https://', rather than just 'http://'.

Tips to follow (4)




If you're using IE, look for the lock symbol in the right of the status bar and double-click it to check the validity of the digital certificate. Or, alternatively, use the telephone to transact your business.

Tips to follow (5)




Consider installing a web browser toolbar that alerts you to known phishing attacks.

Tips to follow (6)




Think about using plain text in your emails, rather than HTML. It may not look as nice, but it's a lot safer

Tips to follow (7)




Check your bank accounts regularly (including debit and credit cards, bank statements, etc), to make sure that listed transactions are legitimate.

Tips to follow (8)




Make sure that you use the latest version of your web browser and that all necessary patches have been installed.

Tips to follow (9)




Immediately report anything suspicious to your bank or credit card provider

Tips to follow (10)



Don't try to investigate the
site on your personal or
company machine

Tips to follow (11)



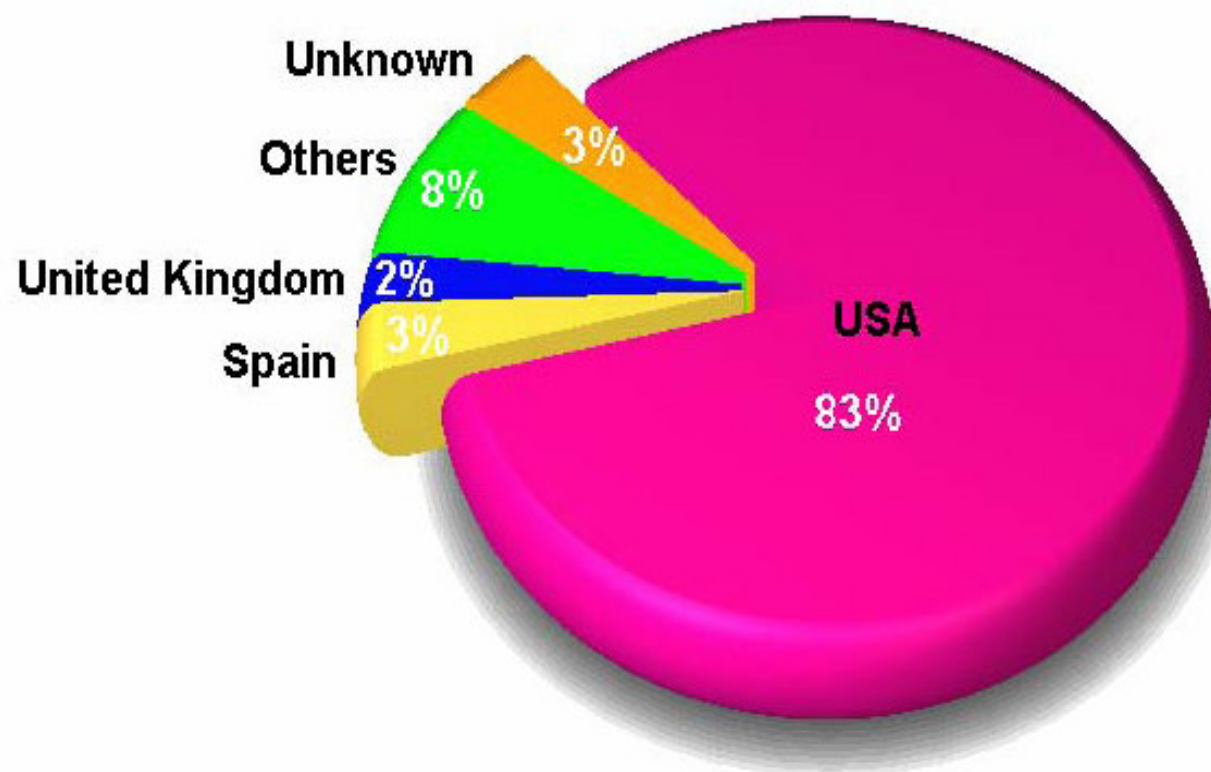
Look for clues that
message is bogus

6. Statistics

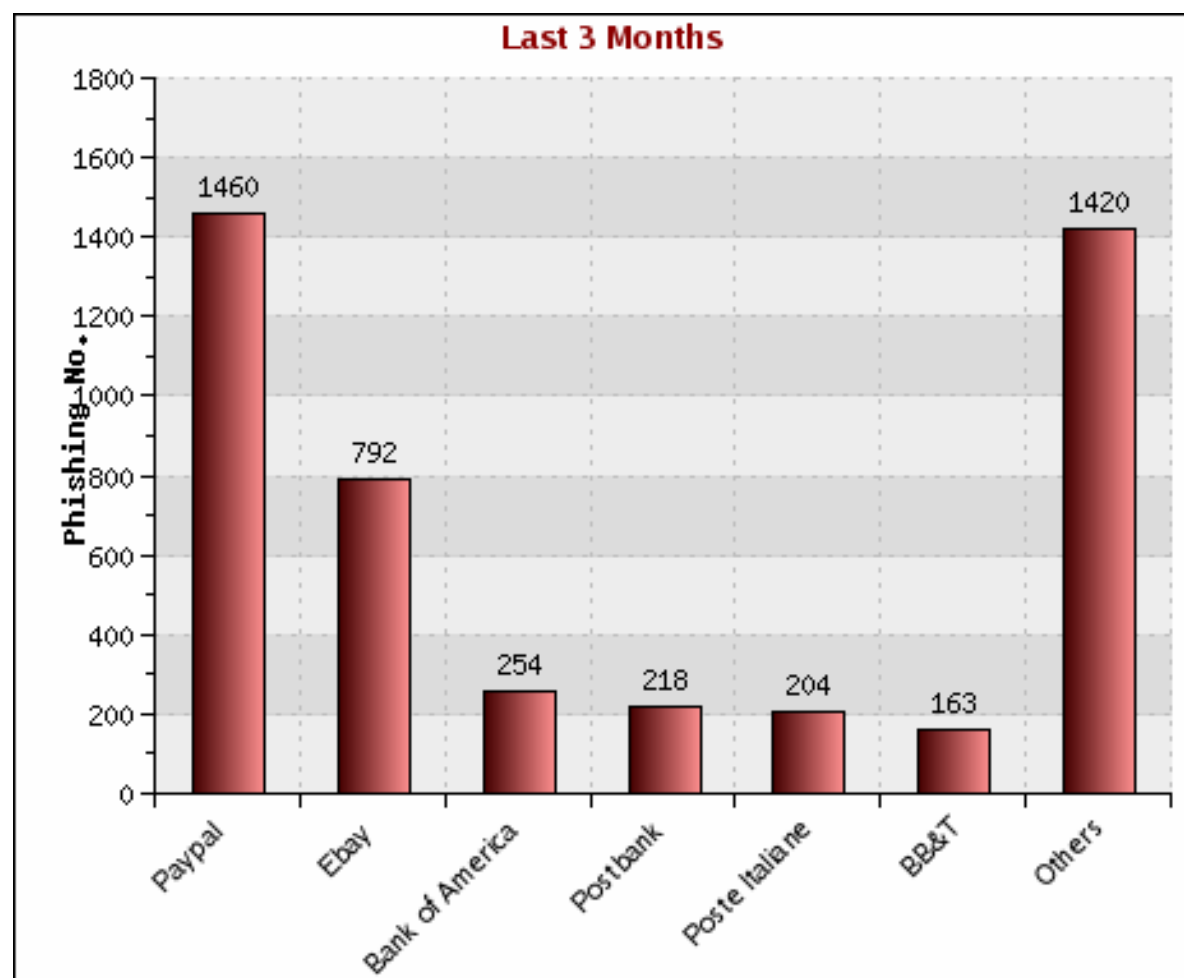
Most-targeted industry sectors



Countries in which hijacked brands belong to



Phishing statistics – top targets



Statistics (1)

- Recent data suggest that phishers are able to convince up to 5% of recipients to respond to their e-mails, resulting in an increasing number of consumers who have suffered credit card fraud, identity fraud, and financial loss.

Statistics (2)

- Most organisations have done very little to actively combat Phishers;
- Phishing scams have been escalating in number and sophistication with every month that goes by.

Do not open the e-mails
you are not expecting!!!