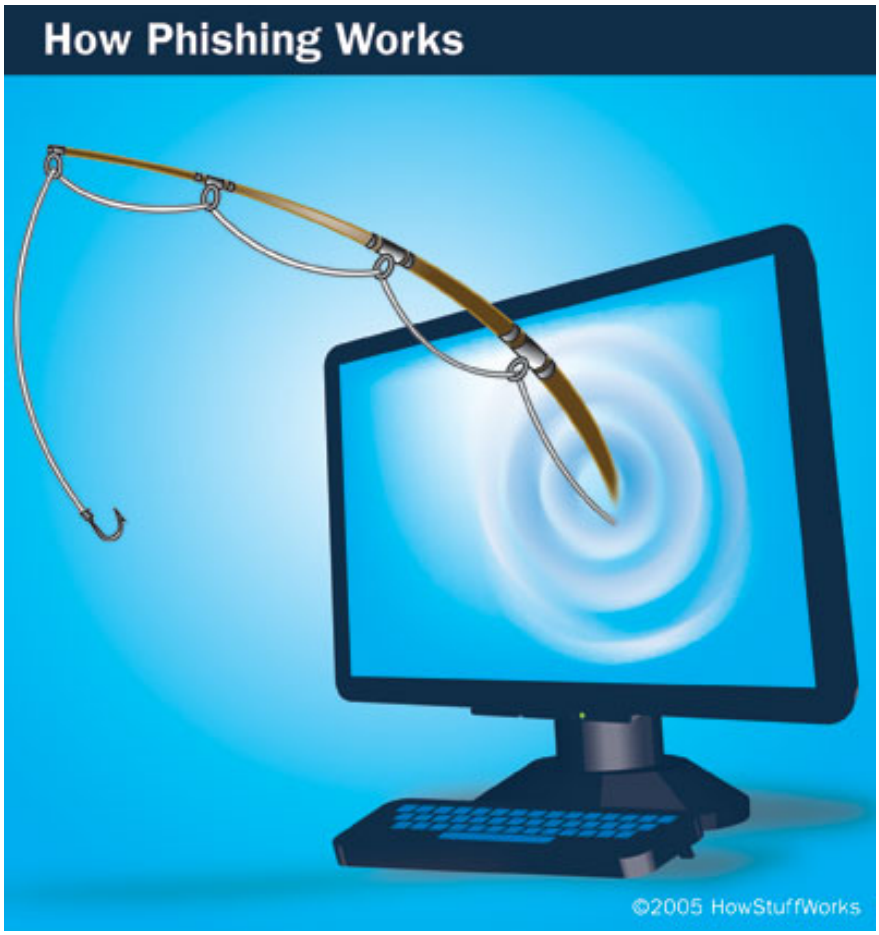
How Phishing works

In the previous post, we learned how to avoid facebook scam. Today, we will learn more about how phishing works.

***TipsMake.com* - In the previous post, we learned how to avoid facebook scam. Today, we will learn more about how phishing works. Suppose one day you open your email and receive a notification from the bank. You have received email from this bank before but this email seems suspicious, especially it requires you to respond immediately or your account will be closed. What you will do?**

>> How Hacker works



Such announcements or similar are examples of Phishing - online fraud, a method of identity theft - to steal personal data. In addition to stealing personal information and financial data, a phisher can infect computers with viruses and convince people to unconsciously engage in money laundering.

Most people encounter online scams with phishing emails or pretending banks, credit companies or businesses like Amazon and eBay. These emails look very real and try to convince all victims to disclose personal information. However, email notification is only a small part of online fraud.

From start to finish, this process includes:

1. Planning : Online scammers determine which business 'deserving' goal is the victim and determine how to retrieve that business's email address. They often use multiple emails and methods to collect email addresses like spammers.

2. Setup : After identifying businesses and victims, phishers will find ways to distribute emails and collect data. Usually, they use an email address and a website.

3. Attack : This is a step everyone knows - phisher will send a fake message, such as from a reliable source.

4. Collect : Phisher will collect information that the victim fills in Web pages or pop-up windows.

5. Stealing personal and phishing data : Phisher uses the information they collect to make illegal purchases or even fraudulent attempts.

If online scammers want to arrange another attack, he will determine the success rate and failure of a successful scam and start the process again.

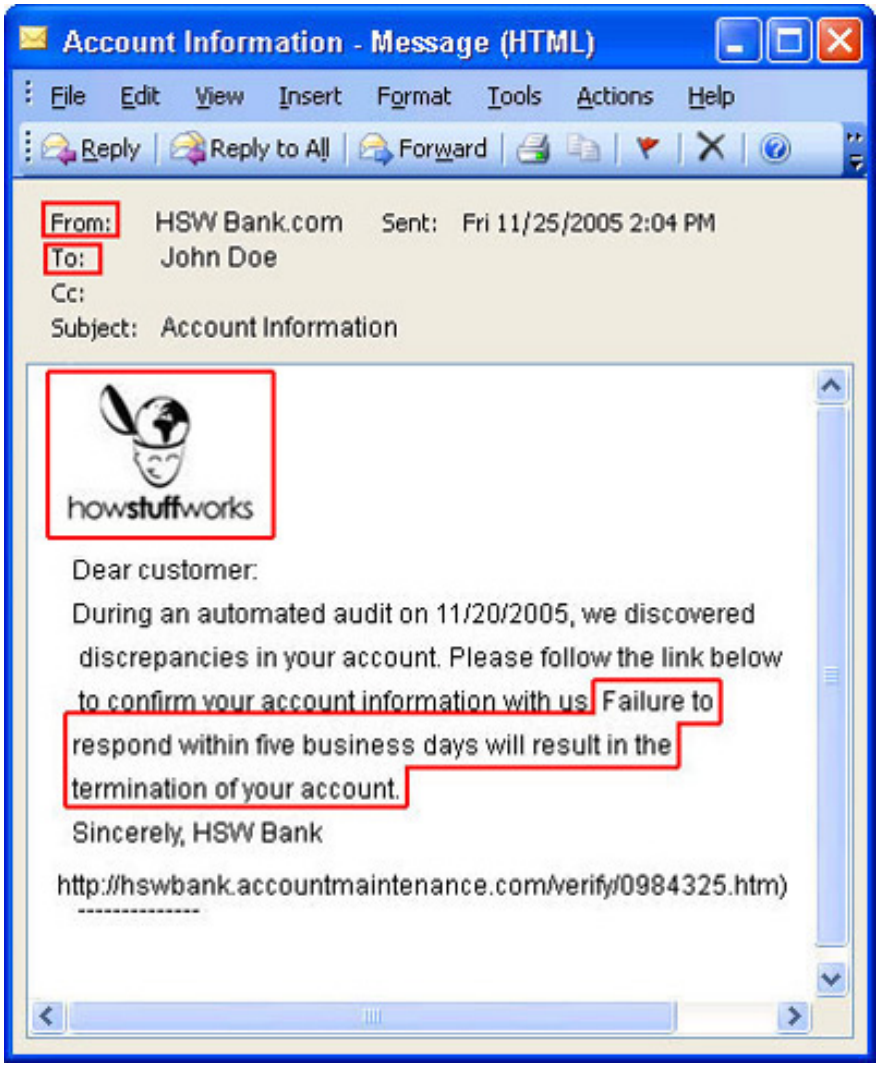
Phishing online

The origin of phishing - online scam

The first document used the word 'phishing' in 1996. Most people assumed that it was derived from salamander pronunciation, meaning 'fishing, to extract information'.

If people do not disclose bank account information, credit card numbers or passwords, the phisher will take extra steps to trick the victim into giving them this information. Scams to get information are called social engineering.

Phisher often uses a company's real logo and copies their legitimate email, replacing the link to lead the victim to their phishing page. They will use fake addresses in the 'From' and 'Reply-to' sections of emails and edit links to make them look more legitimate. However, correcting the appearance of an email is only part of the process.



Most fraudulent messages always give reasons to make the victim act quickly, do it beforehand. These notifications often warn victims that their accounts will be closed if they do not respond quickly. Some cheat victims with sales they have never done. Because victims do not want to lose money that they really do not want, the victim will click on the link and open the door for scammers to get some important information.
In addition, many people believe in automated processes, claiming that they are harmless by humans. That's why a lot of messages claim that computer tests or other automated processes can reveal errors related to the victim's account. The victim is also more likely to believe that someone is trying to break into his account rather than believing that the computer is in error.

Phishing online: not just E-mail

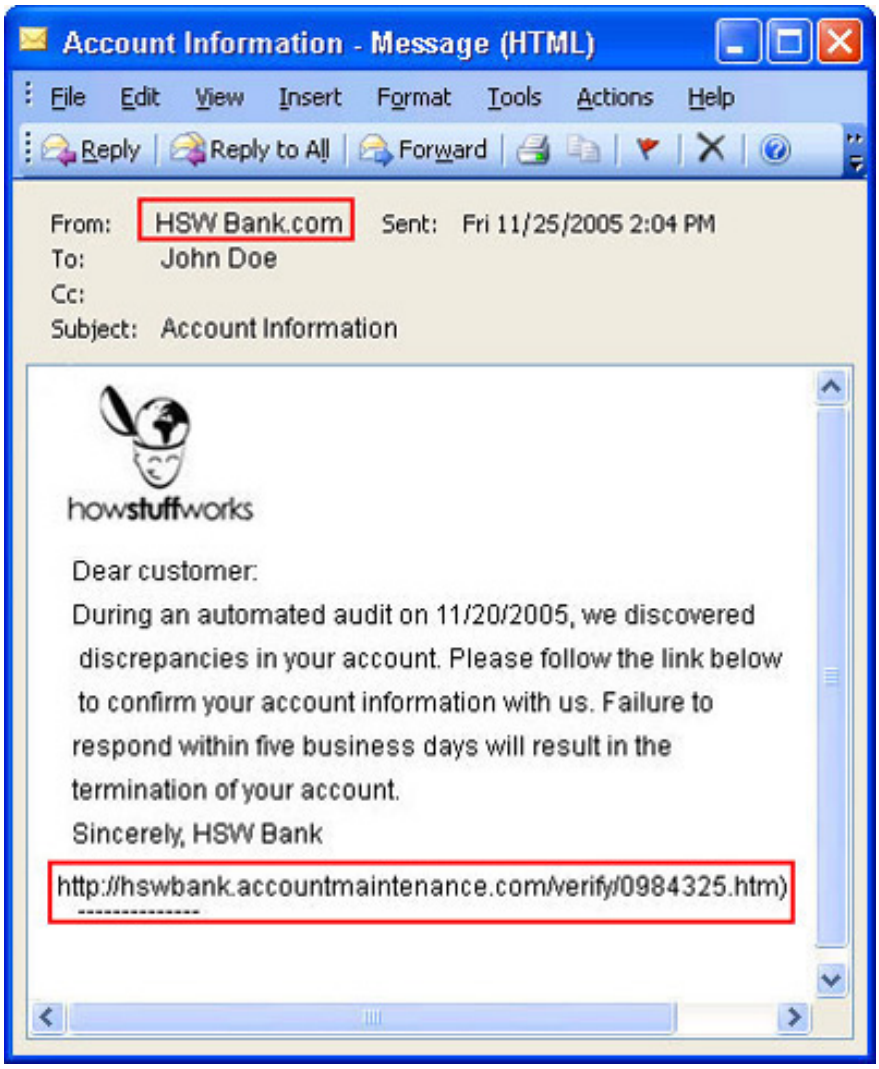
E-mail is the most commonly used way to attract scams. however, some people still search for victims through:

• Instant messages
• Phone citation message
• Chat room
• Fake advertising
• Notification panel and email list
• Fake job search pages
• Fake toolbar in browsers

Next, we will explore ways to create a fake message.

Fake address

The more complex the Web browser and the email client is, the easier it is to find vulnerabilities and weaknesses. This means that online scammers will add tricks to programs to become more and more dangerous. For example, the more effective ways to combat spam and online fraud, the more phisher is cunning to overcome these ways.



The most common way is to use a fake address. Many email programs allow users to enter information in the From and Reply-to sections. While this can be handy when people use multiple emails, this also facilitates online scammers to create an email that looks like legitimate sources. Some email servers allow computers to connect to the SMTP protocol without the need for a password. This allows the phisher to connect directly to the email server and instruct the victim to send a notification to the victim.

Other tricks include:

- **The links are not clear** . These links appear to be actually actually connected directly to the victim's Web site. Some eclipsing skills include:

1. Use a false, fake address of a Web site or use an international domain name to recreate a URL with slightly different characters.
2. Use the company name in the URL but with another domain name.
3. Use the alternate format, like hexadecimal to display the URL.
4. Combine the use of instructions to redirect to reliable URL addresses.
5. Use HTML to display fake links. For example, a link looks like it will lead you to an article, but it actually directs you to all other articles.

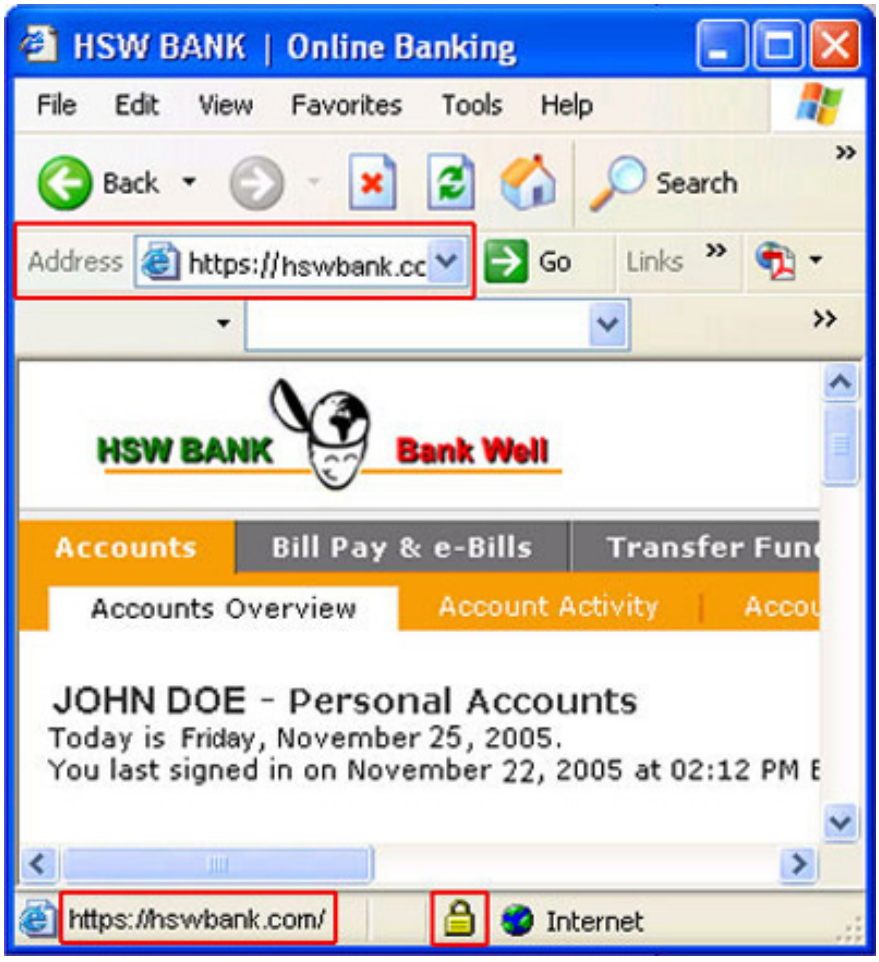
• **Graphics** . By specifying the account and browser that the 'prey' is using, the phisher replaces the image of the address bar and the security key on the real address bar.

• **Pop-up windows and frames** . A pop-up window containing malicious code may appear on the web page you are viewing or the hidden frame around the page may contain malicious code.

• **HTML** . Some phishing emails look like harmless but contain hidden HTML addresses along with links to help this email pass the way the anti-spam program.

• **DNS cache contains malicious code** . Another method is pharming, when the phisher changes DNS server information. This makes people access a fake Web address directly from a certain address. Pharming is difficult to detect and can harm many victims at the same time.

Scammers can use an intermediary victim computer with a Web site to record victims' transactions. They can also take advantage of poorly secured Web sites and malicious code into a certain page. In addition, phishers using these methods will not disguise their links because the Web site they use is a legitimate site, the victim will not have any doubts about their information. will be stolen.



In addition, phisher can use malicious programs in its tricks:

• Trojans help lock keys and take screenshots to record and send notifications to all phishers.

• Trojans remotely access, turning a victim's computer into a medium, phishers use this intermediary to spread other phishing emails or to host a fake Web site.

• Virtual robots make conversations with victims in chat rooms or coordinate a virtual network.

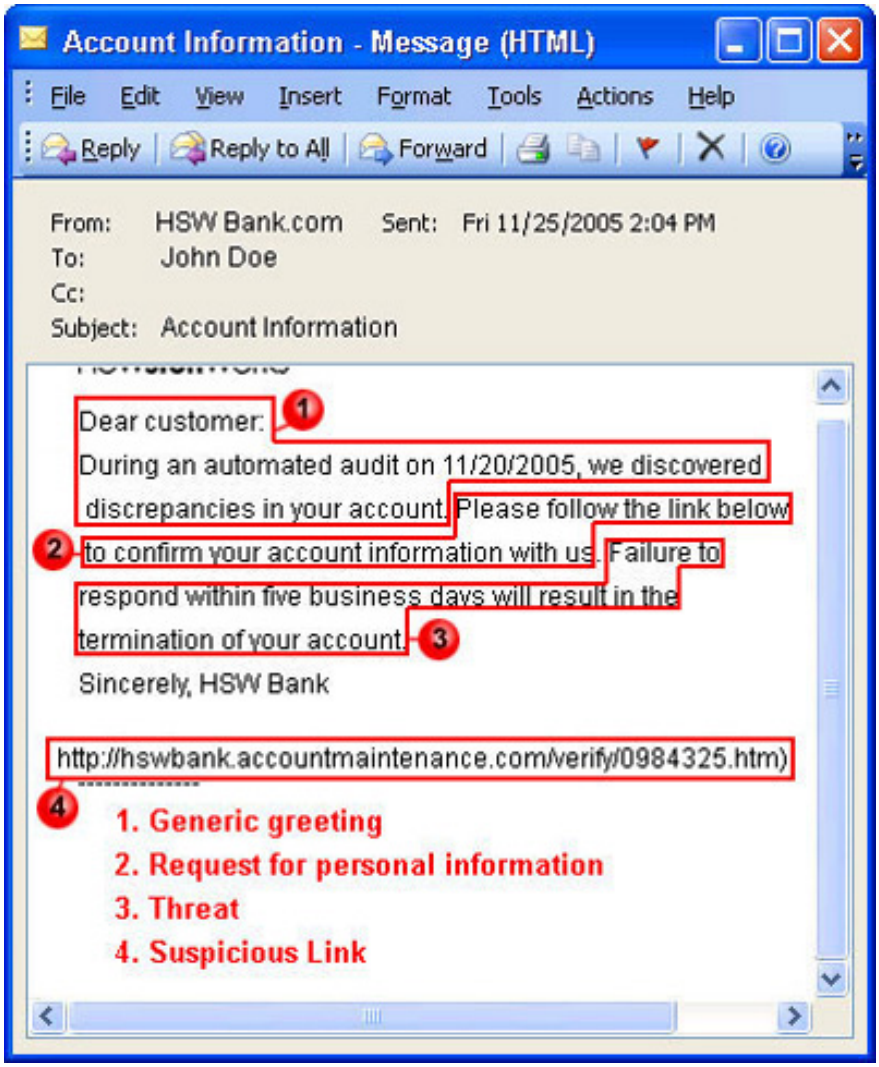
• Spyware tracks and records user activity online, enabling phisher to plan an attack.

Online fraud protection

The steps you usually take to protect your computer, such as using firewalls and anti-virus software, can also help you avoid online scams. You can display the Web site's SSL certificate and the bank or credit card preprint for additional security measures.

In addition, phisher tends to leave some signs in email notifications and Web addresses. When you read the email, pay attention to:

1. General greetings, such as ' *Dear Customer* '. If the bank you are sending money to sends you an official notice, there will be your full name in it (some phishers have recently switched to spear phishing - including your personal information)



2. Threaten your account and ask the user to take action immediately, for example 'reply within 5 days or we will close your account'.

3. Request personal information. Most businesses do not require you to provide personal information via phone or email before online scams become popular.

4. Suspicious links. Longer than normal links, misspellings can also be a sign of online fraud. It is safer if you address the Web site in the browser, rather than clicking on any link in the email.

5. Wrong severe spelling

Fortunately, businesses and governments are still fighting online fraud. At the end of 2006, the US government instructed banks to use security methods, including passwords and methods such as identification cards, fingerprint scanners, for online transactions. Many Internet service providers (ISPs) and programmers have provided phishing tools that help identify security, notify you of the addresses you want to access that have been signed and processed. They also provide phishing notification tools. Other software uses identifiers to confirm that you have accessed a legitimate address.

Data on Phishing

• 13,776 phishing attacks on 5,259 Web sites took place in August 2005.

• They target 84 different businesses but there are 3 businesses that receive 80% of the attack capability.

• 85% of attacks are targeted at banks or financial institutions.

• Phisgher succeeds in stealing personal information from 5% of their victims.

• 57 million Internet users in the US have received phishing emails at least once, and 1.7 million have sent personal information to online scammers.

Facing phishing

If you receive an email that you believe is from phishers, you should not: reply back, click on the link in the email or fill in the personal information. Instead, you should find a way to tell the business that they are spoofing. use their Web site or phone number rather than following links in fake emails.

If you believe you have sent personal information to a phisher, you should send the notice to:

• The company has been forged

• Banks and credit institutions let them close your personal information

• Notice to the nearest police office

In addition, you should change the password at the site where you were recently tricked. If you use a password for multiple Web sites, you should also change the passwords for those sites.