



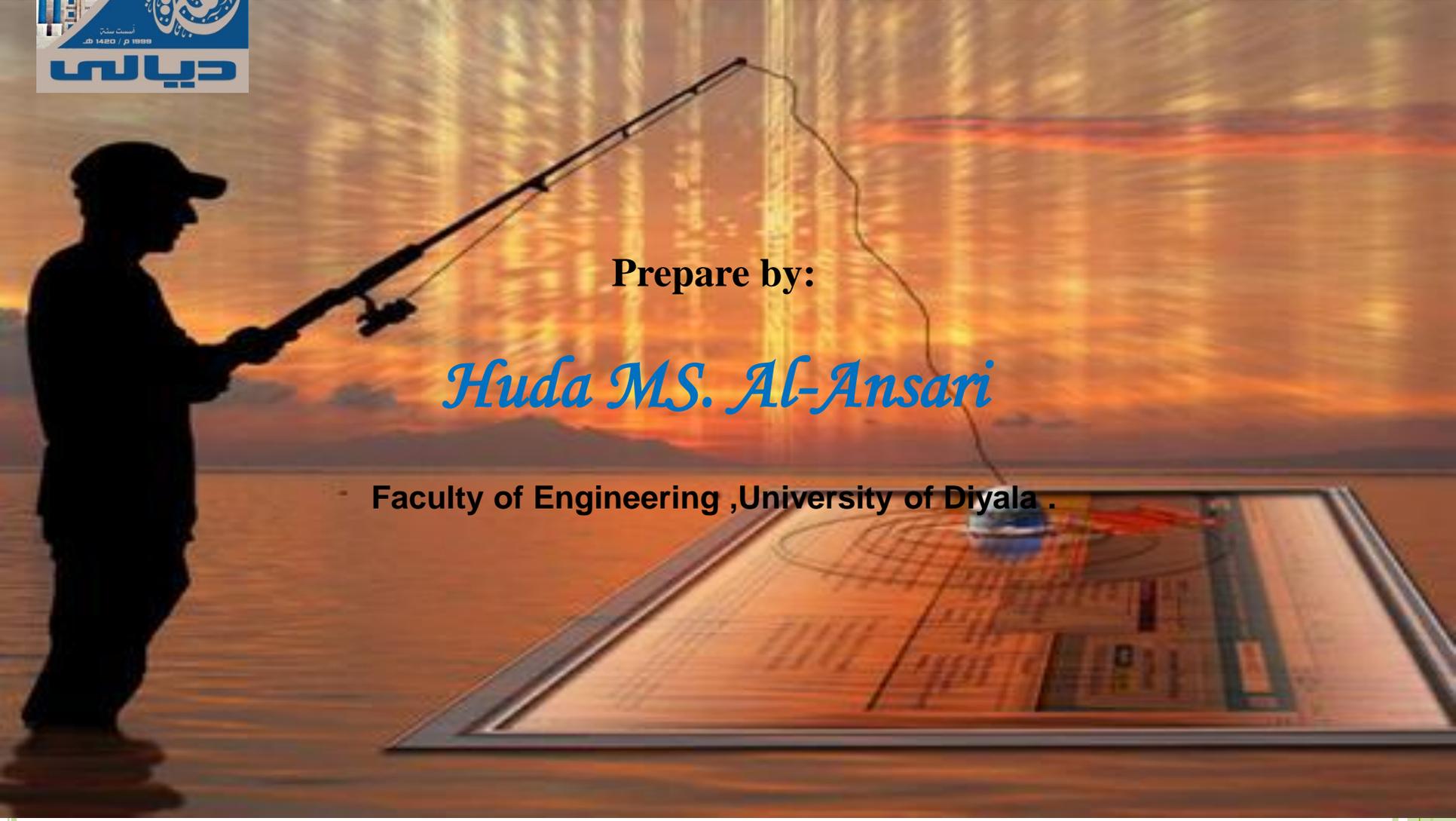
Quick Guides to Scary Internet Stuff (Phishing)



Prepare by:

Huda MS. Al-Ansari

- Faculty of Engineering ,University of Diyala .



Outline

- ✓ *Introduction*
- ✓ *What is phishing*
- ✓ *How phishing works*
- ✓ *Phishing Techniques*
- ✓ *How to Prevent Phishing Scams*
- ✓ *Protection through Software*
- ✓ *How to protect*
- ✓ *briefly*
- ✓ *References*

INTRODUCTION

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as trustworthy entity in an electronic communication .

The word is created as a homophone of fishing due to the similarity of using fake bait in an attempt to catch a victim. Phishing scams use spoofed emails and websites as lures to prompt people to voluntarily hand over sensitive information.

The term “Phishing” is commonly used to describe these ploys . There is also a good reason for the use of “ph” in place of the “f” in the spelling of the term . Some of the earliest hackers were known as phreaks.



WHAT IS PHISHING

- ▶ The term is a variant of fishing and alludes to baits used to "catch" **confidential identity information** such as passwords, and **financial information** such as credit card details -usually via email- by pretending to be a trustworthy company with which the intended victim may have a business relationship; **PayPal**, **eBay** and **large online banks** are most commonly used.
- ▶ A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996.



PHISHING MESSAGE EXAMPLES



Dear Valued Member,

Account Alert

Dear Valued Member,

Due to the congestion in all Yahoo users and removal of all unused Yahoo / be shutting down all unused Accounts, You will have to confirm your E-mail Login Info below after clicking the reply botton, or your account will be susp for security reasons.

UserName:.....
Password:.....
Date of Birth:.....
Country Or Territory:.....

After following the instructions in the sheet, your account will not be interrump normal. Thanks for your attention to this request. We apologize for any inco

Warning!!! Account owner that refuses to update his or her account receiving this warning will lose his or her account permanently.



... you that your eBay account could be suspended if you don't re-update your
...
... item please visit link below and re-enter your account information:

http://www.eBay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

... uld not be resolved your account will be suspended for a period of 24 hours,
... ir account will be terminated.



Dear valued customer of TrustedBank,

We have recieved 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

HOW PHISHING WORKS

▶ 1- Planning.

decide which business to target and determine how to get e-mail addresses for the customers of that business.



ruggia0441c fotosearch.com

▶ 2- Setup.

create methods for delivering the message and collecting the data. Most often, this involves e-mail addresses and a Web page.

HOW PHISHING WORKS

▶ 3- Attack.

This is the step people are most familiar with -- the phisher sends a phony message that appears to be from a reputable source.

▶ 4- Collection.

Phishers record the information victims enter into Web pages or popup windows.

▶ 5- Identity Theft and Fraud.

use the information they've gathered to make illegal purchases or otherwise commit fraud.



PHISHING TECHNIQUES

Phishing is the method used to steal personal information through spamming or other deceptive means. There are a number of different phishing techniques used to obtain personal information from users.

1. Email / Spam.
2. Web Based Delivery .
3. Instant Messaging .
4. Link Manipulation .
5. Session Hacking .
6. Content Injection .

Phishing attacks are trying to steal your money!



HOW TO PREVENT PHISHING SCAMS

A lot of *phishing* emails claim to come from legitimate sources or popular websites. The emails often ask the user to enter bank details or other personal information.

There are also *phishing scam websites* which appear exactly like the original websites. Once the phishers get a hold of the information they can carry out fraudulent monetary transactions.

HOW TO PREVENT PHISHING SCAMS

Sometimes, the website may ask the user to fill in personal details like social security number, driver's license number, and other details which can be used to commit frauds in the user's name .

While *phishing techniques* are getting more sophisticated, there are many things which can access to *avoid phishing*.

- ❖ Here are some of the anti-phishing techniques.

CHECK THE EMAIL CAREFULLY

A *phishing email* may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website.

Sometimes, the link may lead you to the privacy policy of the legitimate company or some irrelevant pages. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with “Dear Customer” so you should be alert when you come across these emails.

You should know that a legitimate company will not send spam emails.

NEVER ENTER FINANCIAL OR PERSONAL INFORMATION

Most of the *phishing emails* will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails.

✓ Never Send Personal Information through emails

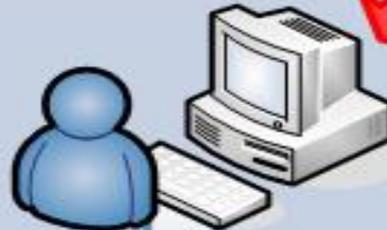
Never send an email with sensitive information to any one. Make it a habit to check the address of the website. A secure website always starts with “https”.

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.



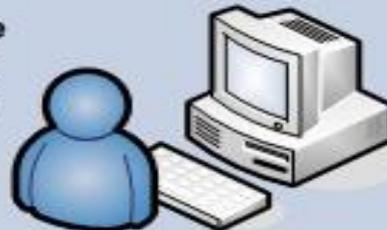
The link in the email directs the user’s web browser to a fake website operated by the hacker.



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.



Phisher



Compromises a host
and installs a phish Web site
and mass-mailer



Victim Web Server

Opportunities to Block:

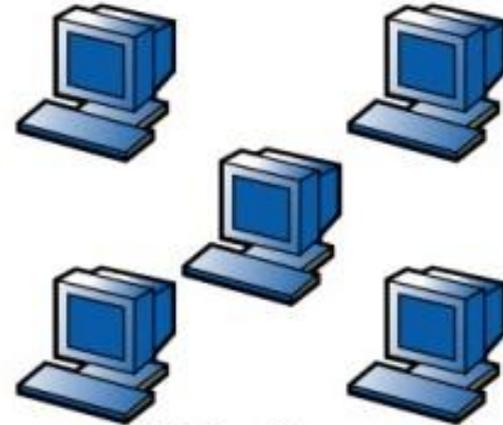
1. Initial Web Site Compromise
2. Mass Phishing E-Mail
3. Victim Clicks on Misleading URL
4. Phish Web Site is Displayed
5. Victim Submits Account Information

Sends out phishing e-mail

Victim clicks a phish URL

Phish Web site is viewed

Victim submits information



Victim Users

PROTECTION THROUGH SOFTWARE

Anti-spyware and *firewall* settings should be used to prevent phishing attacks and users should update the programs regularly . Firewall prevents access to malicious files by blocking the attacks.



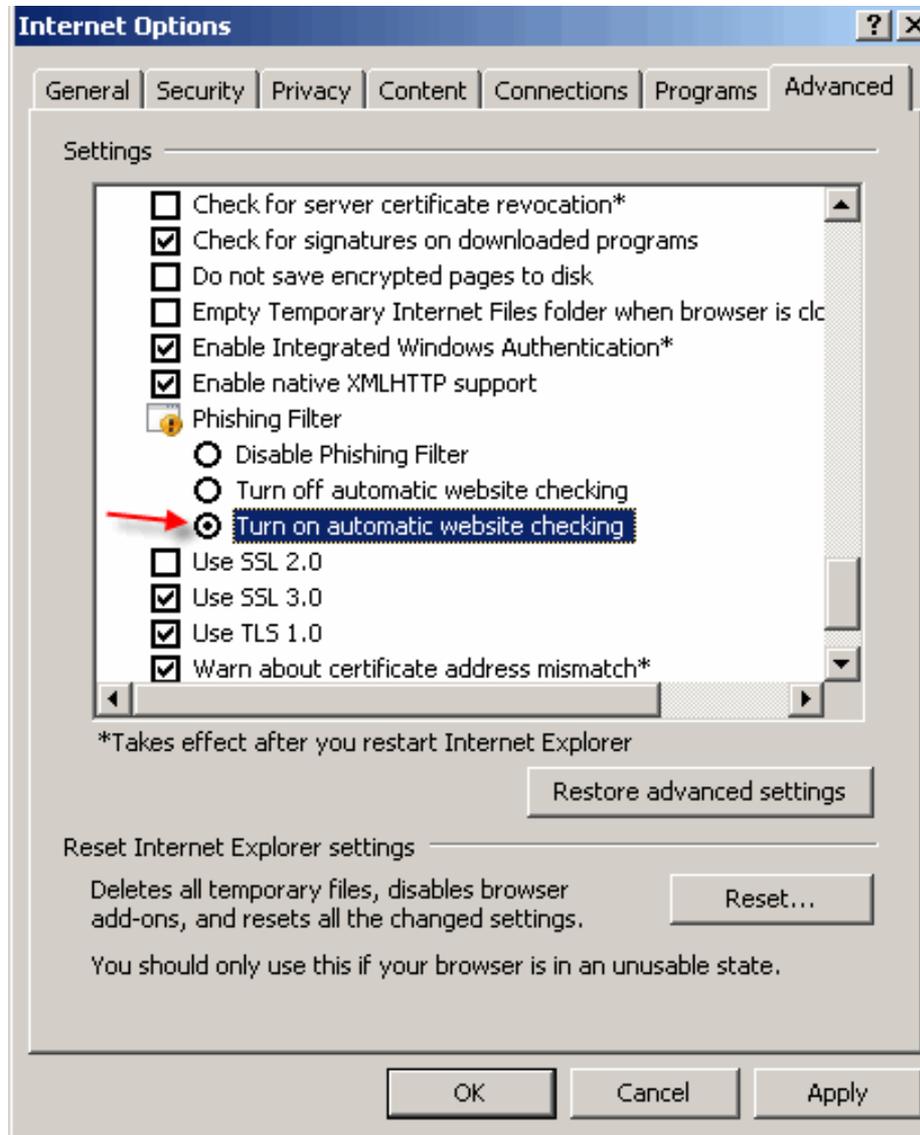
CHECK BANK DETAILS REGULARLY

To prevent *bank phishing* and *credit card phishing scams* you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

✓ Never Download Files from Unreliable Sources

If you get a message stating a certain website may contain malicious files, do not open the website.

Web browsers provide settings to prevent access to malicious web pages and when you try to access a malicious site, an alert message will appear.



[10] Woodgrove Account Violation

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next

From: Account Notice
Date: Wed, 8 Sept 2004 12:41p
To:
Subject: [10] Woodgrove Account Violation



Dear valued Woodgrove member,  **Graphic from bank's actual web site**

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information

<https://vault.woodgrove.com/default.asp> 1

<http://203.144.234.138/us/index.html> 2

LIVES:  TIME LEFT: 0:31



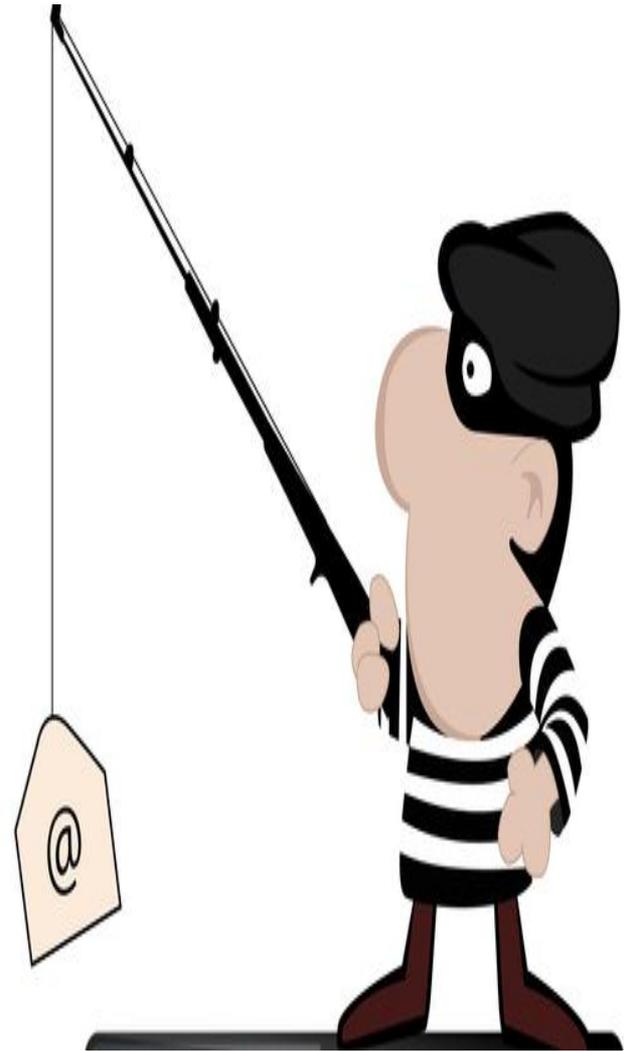
Don't trust URLs with all numbers in the front.

<http://80.157.192.106/www.bankofthewest.com>

R REJECT PHISHING URLS **T ASK YOUR FATHER FOR HELP**

HOW TO PROTECT

- ▶ Never trust strangers
- ▶ Sidestep those links
- ▶ Use the keypad, not the mouse
- ▶ Fear Not
- ▶ Guard your privacy
- ▶ Second time right
- ▶



- ▶ [44 ways protect phishing](#)

BRIEFLY





Thank You for listening
Any Question!

QUESTIONS



REFERENCES

- ▶ [Phishing .. wikipedia](#)
- ▶ [Phishing definition](#)
- ▶ [how phishing works](#)
- ▶ [44 ways protect phishing](#)
- ▶ [Using Social Networks to Harvest Email Addresses](#)
- ▶ [Bad Emails](#)
- ▶ [phishing examples](#)