Phishing

What is Phishing?

- Phishing scams are typically fraudulent email messages or websites appearing as legitimate enterprises (e.g., your university, your Internet service provider, your bank).
- These scams attempt to gather personal, financial and sensitive information.
 - Derivation of the word "phishing".

- Phishing a kind of deception in which an attacker pretends to be someone else in order to obtain sensitive information from the victim
- Also known as "brand spoofing"

- Phishing "IDENTITY THEFT" is obtaining sensitive
 & valuable information about the customer.
- Phishing makes high profit with less or small tecnological investment.
- It tries to **trick** users with official-looking messages

Some phishing **e-mails** also contain malicious or unwanted

software

Types of phishing

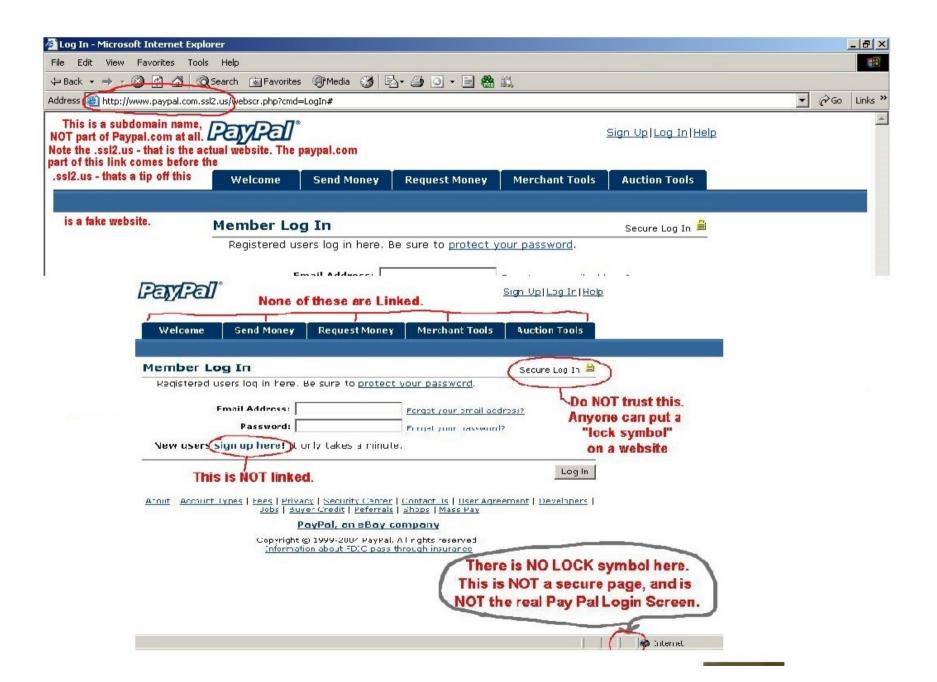
- Mass phishing attacks
- An attacker sends out deceptive emails, which appear to be from a legitimate organisation, to a significant number of email addresses.
- The aim is to convince some proportion of the recipients to click on an embedded link in the message that directs them to a malicious website masquerading as a legitimate one.
- More recent versions of this attack do not try to persuade the user to divulge information, but rather to persuade them to perform some action. This could be visiting a website that downloads malware through a software vulnerability on the user's machine, or opening an email attachment that contains malware

Spear phishing attacks

- Spear phishing is a highly targeted attack against a small group of individuals.
- It uses prior knowledge of the organisation or individual to construct an approach that is far more likely to elicit the intended response.
- Spear phishing attacks often target high profile individuals within organisations who typically have extensive or deep access to sensitive information

Email Message

```
Subject: CONFIRM YOUR ACCOUNT
     Reply-To: "CLEMSON.EDU SUPPORT TEAM"
From: "CLEMSON.EDU SUPPORT TEAM"
П
        Date: Tue, 1 Dec 2009 17:42:05 -0400
          To: <"Undisclosed-Recipient:;"@iocaine.uits.clemson.edu>
П
Dear CLEMSON.EDU Webmail user,
           This mail is to inform all our {CLEMSON.EDU } webmail users that we
will be maintaining and upgrading our website in a couple of days from now to a
  new link. As a Subscriber you are required to click on the link below and login
  to check if you have access to the new link.
Click Here: www.webmail.clemson.edu
П
      Failure to do this will immediately will render your email address
deactivated. Thank you for using CLEMSON.EDU.
      CCIT SUPPORT TEAM
```



POPULAR FRAUDULENT EMAIL PHRASES

"Verify your account."

*** If you receive an e-mail from Microsoft asking you to update your credit card information, do not respond: this is Phishing scam.

"If you don't respond within 48 hours, your account will be closed."

"Dear Valued Customer."

"Click the link below to gain access to your account."

• How to phish?

- Compromised Web servers Email and IM
- □Port Redirection
- Botnets
- Key loggers

How to avoid Phishing

- DON'T CLICK THE LINK
 - -Type the site name in your browser (such as www.paypal.com)
- Never send sensitive account information by e-mail
 - Account numbers, SSN, passwords
- Never give any password out to anyone
- Verify any person who contacts you (phone or email).
 - -If someone calls you on a sensitive topic, thank them, hang up and call them back using a number that you know is correct, like from your credit card or statement.