Social Engineering

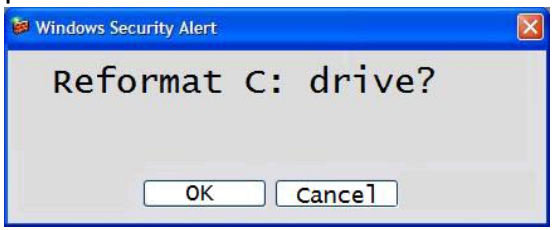
COMP620

Social engineering

- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques
- Similar to a confidence trick or simple fraud

Users Often Make Bad Decisions

- Many naive users will OK anything
- Many users have insecure passwords
- Most users do not know how to protect their computer



Phishing

- Phishing is the criminally fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity
- Targeted versions of phishing have been termed **spear phishing**

Damage Done by Phishing

- One study estimates that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by phishing, totaling approximately US$929 million
- Businesses lose an estimated $2 billion per year as their clients become victims
- Microsoft claims the loses are only about $60 million a year

Phishing Works

- A 2005 study showed that about 19% of all those surveyed reported having clicked on a link in a phishing email
- Even if only one out of a million users fall for the fraud, that will give you 10 victims if you send out 10 million emails.

Social Engineering on Social Networks

- Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft
- In late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details
- Experiments show a success rate of over 70% for phishing attacks on social networks.

Email Phishing

```
I am the son of a late Nigerian
banker.  I have inherited the sum of
$40 million dollars which I need to
transfer to an account in a U.S.
bank.  If you would assist me in
transferring these funds, you would
be rewarded with 10% of the amount.
Just send me your account number and
I will transfer the money to your
account.
```

Email Phishing

The First National Bank is implementing new security features. To keep your account safe, please reply to this email giving:

your account number: _____

your password: _____

You will not be able to access your account in the future unless you provide this information.

More Convincing Email Phishing

TrustedBank™

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 discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Email Links

- The URL shown in an email link does not have to match the URL used when you click on the link

```
<a href="http://www.evil.com">
www.nice.com</a>
```

- This displays as

www.nice.com

- In the lower left hand corner of most browsers you can preview and verify where the link is going to take you

Ken Williams' Opinion

- Browsers and Email systems should warn users when the displayed link does not match the actual URL

Website Forgery

- It is easy to copy the content of a real website and put it on your own fake website
- If the fake website has a digital certificate, it will validate under HTTPS

Man in the Middle Attacks

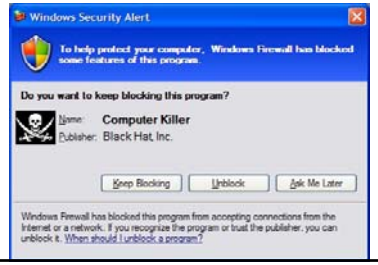
- A false website can redirect all of the traffic to the true website after recording accounts and passwords
- A Universal Man-in-the-middle Phishing Kit, discovered by RSA Security, provides a simple-to-use interface that allows a phisher to convincingly reproduce websites and capture log-in details entered at the fake site

Countering Phishing

- Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures
- User education is the primary solution
- The secure site “padlock” is becoming more obvious

Click Through Syndrome

- Many users will allow a dangerous event to occur because it appears necessary to make the activity work
- This is exacerbated by poorly managed honest sites that have certificate problems



Augmenting password logins

- Some sites display a personalized phrase when you are asked to enter your password
- If you do not see the correct phrase, you should not enter your password.
- The sites IP address can be used as part of the user authentication

Legislation

- Federal laws have been proposed to fight phishing
- The Anti-Phishing Act of 2005 was introduced in Congress on March 1, 2005

Legal Remedies

- In January 2007 the first person was convicted by a jury under the provisions of the CAN-SPAM Act of 2003.
- He was found guilty of sending thousands of e-mails to America Online users, while posing as AOL's billing department