

## **Informative Newsletters on Information Security**

### **Phishing Scams**

#### **WHAT IS PHISHING?**

- A criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- Most attempts will entice email recipients or instant messenger users into clicking on a link that takes them to a bogus website
- The bogus website may prompt the recipient to provide personal information such as bank account number, passwords and/or it may download malicious software onto the recipient's computer
- Both the received link and bogus website may appear authentic, however they are not legitimate
- In the past, phishing scams were often more easily detectable because of misspellings, typographical errors and blatantly bad grammar. Nowadays they are increasingly more difficult to detect because they often appear so legitimate
- The types of messages used in phishing are expanding almost every day, so it is important to be cautious of any communications you receive

#### **PHISHING TECHNIQUES**

- Sent via an email, an instant message, or another communication that appears to be from a reputable organization
- The malicious email could include notice of an account cancellation, a request to verify/update personal information, warning users of suspicious activity on their account or just about anything else that would get you to respond to the communication
- Users may be "tricked" into visiting a website, which appears to be a legitimate organization's website. Once at that site, users may be asked to enter personal information
- Other variations include a telephone call, in which the phisher will ask you to provide personal information
- Once the phisher has "hooked" you, they may use the information to open accounts in your name and access your bank account

#### **HOW DO YOU KNOW IF IT IS a PHISHING SCAM?**

- If you receive an email appearing to be from a legitimate business, requesting you submit personal information, it is most likely a scam. Legitimate businesses do not send emails requesting personal information
- Use an Internet search engine to research the subject line of a suspicious email to determine if that subject line is a known phishing scam

#### **PROTECTING YOURSELF FROM PHISHING SCAMS**

Do not reveal any personal information in e-mail, online or on the telephone unless you know who you are dealing with and why. Additionally, make sure you are in a secure environment:

We can fight Phishing Scams by following common sense guidelines:

- Be cautious about all communications you receive. Think before you click
  - If the communication appears to be a phishing communication, do not respond. Delete it.
-

- Do not click on any links listed in the email message and do not open any attachments contained in suspicious email
- Do not enter personal information in a pop-up screen. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens
- Internet-Banking Applications: **VISIT SITES DIRECTLY**, if you need to enter your account details, only go there by typing the site's address directly into the browser. Don't trust any web link you received
- When logging onto the Internet Banking Service, look for the security certificate before entering the User ID and Password. To view the security certificate, click on the 'Lock' icon at the bottom of the page if you are using Internet Explorer. Be sure that the website is using **HTTPS** protocol not **HTTP** in the address bar
- Read carefully the internet banking service **disclaimer** before logging onto your account
- Install a phishing filter on your email application and also on your web browser. These filters will not keep out all phishing messages, but will reduce the numbers of phishing attempts
- Ensure that your computer is up-to-date on all patches
- Ensure that your antivirus program is installed and up-to-date
- Use bookmarks in your web browser for the organization's which with you regularly communicate to limit the chances of being redirected to malicious sites
- Use strong passwords for your bank accounts: avoid easily guessed passwords such as your birthday, your address, etc.
- Do not store your bank account IDs and Passwords on a file on your computer or write them down on a paper
- Review your credit report regularly and look for unauthorized charges or withdrawals on bank statements/bills

**Figure 1 (How Capital Bank's Internet Banking Website Should Look Like)**

