Scam and Fraud Education

Your personal space. Nothing should violate it, least of all someone seeking to profit from you through financial fraud and abuse. Here is some helpful information on how you can spot scams, particularly “phishing” and “spoofing” attacks, and protect yourself from fraudsters seeking your personal financial information.

What is “Phishing”?

"Phishing" is a scam that uses fraudulent emails to falsely solicit personal financial information. The emails stress urgency and threatens dire consequences if you do not respond via email or click an embedded link to then provide private information. Always be suspicious of any email with requests for personal financial information.

Spotting “phishing” attacks:

- **Requests for personal or financial information.** Legitimate companies like United Bank do not ask for this type of information via email for any reason - to update their records, keep your account open, update security, or to send you money in return for completing an online survey.
- **Sense of urgency.** Emails containing statements that imply that your account will be closed if you don't respond shouldn't be opened.
- **Obvious spelling errors** either in the body of the email or in the URL are purposeful to help avoid spam filters.
- **Questionable links.** If you mouse over a link (but do not click on it) your email program will most likely show the full destination URL. Typos or slight variations in the company's web address may tip-off that the link is not legitimate.

How you can protect yourself from “phishing”:

- Regularly log on to your online accounts and review your transaction history.
- If you suspect an email or pop-up message might not be authentic, don't click "respond" or an embedded link. If the email in question looks like it came from United Bank, you can call our Customer Care Center to confirm the message's veracity.
- Ensure that your browser is up to date and security patches are applied. If you use Microsoft Internet Explorer, visit www.microsoft.com/security to download special patches related to "phishing" scams.
- Do not bank using public or shared computers.
- If you suspect that you have been directed to a false United Bank website, or if you are receiving fraudulent emails or phone calls claiming to be from United Bank, Report it!

What is “Spoofing"?

Spoofing is the use of a website or email that appears to come from a well-known company but is fake. For example, an Online Banking customer who routinely logs in to an online banking website may be redirected to an illegitimate web page which looks just like the real website. These spoofed websites are then used to obtain your personal financial information.

Spotting "spoofed" websites.

- **Questionable links.** If you mouse over a link (but do not click on it) your email program will most likely show the full destination URL. Typos or slight variations in the company's web address may tip-off that the link is not legitimate.
- **Static domain name spoofing.** The "pharmer" (the person or entity committing the fraud) attempts to take advantage of slight misspellings in domain names to trick users into inadvertently visiting the pharmer's web site. For example, a pharmer may redirect a user to anybnk.com instead of anybank.com - the site the user intended to access.
- **Malicious software (Malware)**. Viruses and "Trojans" (latent malicious code or devices that secretly capture data) on a consumer's personal computer may intercept the user's request to visit a particular site, such as anybank.com, and redirect the user to the site that the pharmer has set up.
- **Domain Name Servers (DNS) poisoning**. The most dangerous instance of pharming may be DNS poisoning. Domain name servers are similar to Internet road map guides. When an individual enters www.anybank.com into his or her browser, DNS on the Internet translate the phrase anybank.com into an Internet protocol (IP) address, which provides routing directions. After the DNS server provides this address information, the user's connection request is routed to anybank.com. Local DNS servers can be "poisoned" to send users to a website other than the one that was requested. This poisoning can occur as a result of misconfiguration, network vulnerabilities or Malware installed on the server.
- **Man-in-the-Browser or Man-in-the-Middle scams.**These are methods used by cyber criminals to intercept and modify information between two parties. You can protect yourself by not using public or shared computers and always log off if you find yourself waiting for more than a few seconds to get onto a financial site or into your account.

How you can protect you and your business from fraud and identity theft.

The Do's.

- Report any lost or stolen ATM/Debit Card or lost or stolen personal checks.
- Regularly review credit card statements and balance your checking or savings account statement every month and report any unauthorized transactions immediately.
- Shred your charge receipts, credit card applications, insurance forms, old checks, bank statements, anything that contains any of your personal identification.
- Use dual approval controls for money movement or administrative changes.

The Don'ts.

- Never use an unsecured network or a shared computer.
- Never share your Personal Identification Number (PIN) or password.
- Never give out personal information such as your checking or savings account number, credit card number or social security number, through the mail, telephone or Internet, unless you have initiated the contact.
- Never log on using someone else's credentials.

If you're a victim of identity theft or online fraud:

- Call the ID Theft Clearinghouse toll free at 1-877-438-4338 to report the theft.
- Contact the fraud departments of each of the credit agencies:
  Equifax http://www.equifax.com/ 1 (800)-525-6285
  Experian http://www.experian.com/ 1 (888)-397-3742
  TransUnion http://www.transunion.com/ 1 (800)-680-7289
- Contact United Bank and your credit card companies immediately to stop access to your accounts.
- Stop payment on fraudulent transactions or stolen checks.
- File a police report with your local police department or the police in the community where the identity theft occurred.
- Report all suspicious contacts to the Federal Trade Commission: www.ftc.gov/idtheft