

Phishing - Don't Get Caught!



What is "Phishing"? Phishing is an e-mail or other communication impersonating a legitimate organization and trying to get you to volunteer personal information such as bank account numbers or e-mail passwords. Phishers often impersonate banks, PayPal, eBay, credit card companies, and computer Help Desks. Often phishers say there is something wrong with your account, and supplying the information will help them fix it — but it's a **SCAM!** In addition to e-mailed phishing attempts, you may encounter phishing on Facebook, MySpace, Twitter, instant messages, legitimate websites, and even phone calls.

What happens with phished information? Your personal information in the wrong hands can do a great deal of damage, both to you as an individual and to our campus computer systems. It can be used for a variety of fraudulent purposes, such as

- Withdrawing funds from your bank account
- Charging purchases to your credit card
- Opening new credit accounts in your name and charging to the limit
- Using your e-mail account to launch more spam/phishing attacks. The e-mail servers can get so flooded with the resulting spam that service can be very significantly impaired. Successful phishing incidents have actually resulted in e-mail delays on our own campus, impacting everyone's ability to receive timely e-mails and do their jobs effectively. Many colleges, universities, businesses, and other organizations around the country are struggling to control this growing problem.

How do I protect myself?

To protect yourself and our campus community:

- Be suspicious of any communication that asks for personal information such as account numbers or passwords, especially those that threaten your account is closed, that you have won a prize, etc.
- Never respond to e-mailed phishing attempts — just delete as spam.
- Never click on website links provided, asking you to go to a particular website.
- Always double-check the true identity of anyone asking for sensitive information. Use Google or your account statements to find legitimate web addresses of the organization that appears to be sending the communication.
- Keep in mind that communications from UIndy Information Systems will always be signed by an employee, and staff will **never** ask you for your password.
- Keep your anti-virus software up-to-date.
- **Additional information on recognizing and dealing with phishing** is available at <http://is.uindy.edu/faq> - Viruses, Spyware, & Computer Health section.

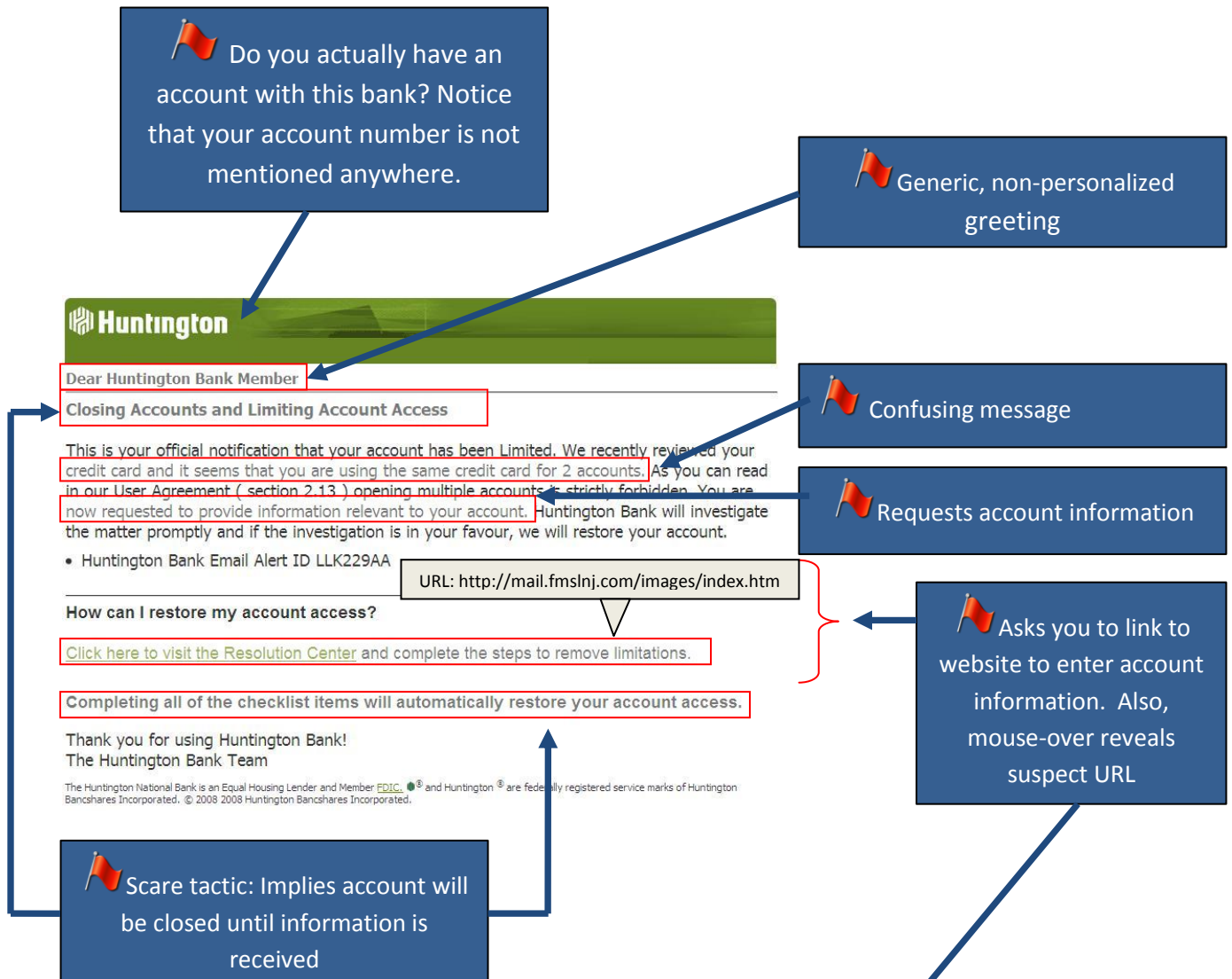
Phishing Facts *

- **886** - The average dollar loss per Phishing Victim (Gartner, Dec 17, 2007)
- **3.6 Billion** - The total dollar loss of all phishing victims over a 1 year period (Gartner, Dec 17, 2007)
- **3.2 Million** - The number of people who fell victims to phishing scams over that same 1 year period (Gartner, Dec 17, 2007)
- **8.5 Billion** - The estimated number of phishing e-mails sent world-wide each month (SonicWALL, 2008)
- **32,414** - The number of phishing web sites that were operational in May 2008 (Anti-Phishing Working Group)

* from <http://www.sonicwall.com/phishing/> accessed on 12/12/08

How to Catch a Phish

The **red flags** indicate this may be a Phishing attempt!



Never click on a link like this! In this particular case, the link provided takes you to an unsecured website asking for a full menu of your personal information, including credit card account number and password, social security number, and mother's maiden name. This information could be used for all kinds of fraudulent purposes, from raiding your bank accounts to ruining your credit by opening dummy accounts in your name. Information about your e-mail password can give hackers the entry they need to launch more cyber-attacks from our UIndy computer servers. The resulting flood of e-mails leaving our system can seriously impair delivery of legitimate e-mail to our campus community.

Anatomy of a Phish

The **red flags** indicate this may be a Phishing attempt!

From: enroll@usbanks.com
To: tbusch@uindy.edu
Sent: Tuesday, December 9, 2008 9:26:11 AM GMT -05:00 US/Canada Eastern
Subject: US Bank - Verified by Visa Enrollment

Dear US Bank Customer }

Your US Bank card has been **automatically enrolled in the Verified by Visa program** }

To ensure your Visa card's security, it is important that you protect your Visa card online **with a personal password. Please take a moment, and activate for Verified by Visa now.** }

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and **create your personal password.** }
You'll get the added confidence that your Visa card is safe when you shop at participating online stores.


Please click the link below Activate Now for Verified by Visa


<http://ngg.ro/usbank/>


We present our apologies and thank you for co-operating. Please do not answer to this email - follow the instructions given. These instructions have been sent to all bank customers and it's obligatory to follow.


@ 2008 US Bank Service Department


*** Please note: If you FAIL to update your Visa card, it will be temporarily disabled.**


 Do you actually have an account with this bank? Notice that your account number is not mentioned anywhere, and this is a generic greeting

 Is this a legitimate VISA program? Checked VISA website and found out it's a real program, making this phish harder to detect!

 Password creation could be just a ploy to get you to enter your account number

 Suspect URL -- the "ro" in this URL indicates an address in Romania. Use Google or your bank statement to verify legitimate US Bank address.

 Strange word choices.

 Scare tactic: Threats of negative consequences if you don't comply.