

Internet Security FAQ

Your security is important to us. Here at Wells Bank we want to provide tools and resources to help prevent identity theft and educate you on security.

➤ **What is “Phishing”?**

- Phishing is a high-tech scam that uses spam or pop-up messages to attempt to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, and/or other sensitive information.

➤ **Protect yourself from “Phishing.”**

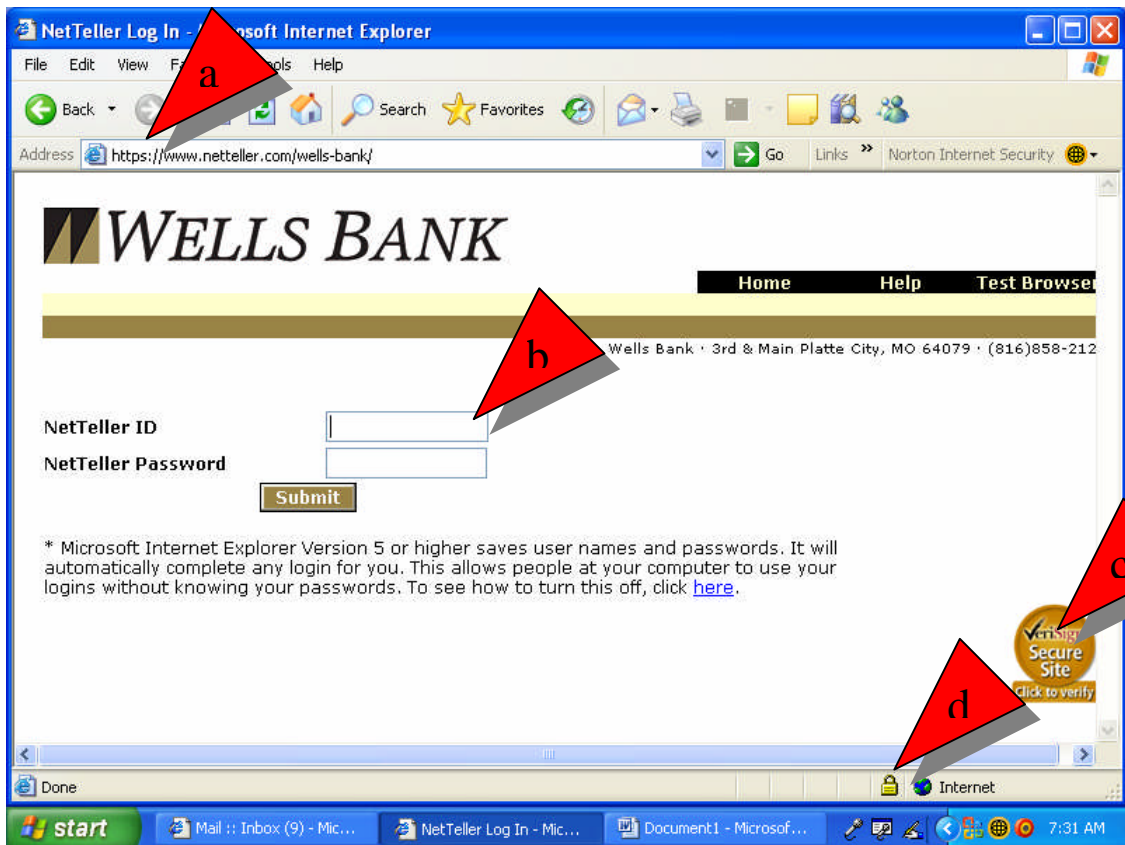
- Wells Bank will never contact you via e/mail or telephone and ask you for your username or password. If we need to contact you, we may ask you for information about your account or personal information to verify your identity. If you ever doubt the source of such a call, you may always insist to call the bank directly at 816-858-2121.
- Do not complete forms in email messages that ask for personal financial information? Wells Bank will never ask you to complete such a form within the body of an e-mail message.

➤ **What is “Pharming” or “Spoofing”?**

- “Pharming” refers to the redirection of an individual to an illegitimate Web site through technical means. For example, an Internet banking customer, who routinely logs in to his/her online banking Web site, may be redirected to an illegitimate Web instead of accessing his or her bank's Web site.
- “Spoofing” is pretending to be something it is not, on the internet, usually an email or Web Site.

➤ **Protect yourself from “Pharming” or “Spoofing”.**

- Here are some things to check for before entering your username and password.



- a. Be sure to check the url before entering your username and password. The “s” at the end of “https” indicates the web site you are viewing is secure.
- b. Check your computers settings and turn off *saving usernames and passwords* if this feature is turned on.
- c. You can also click here check the validity of the web site.
- d. When you see this padlock, it means you are on a site with 128 bit SSL (secured socket layer) encryption.

➤ **Consumer Tips**

- Never give out you personal financial information in response to an unsolicited phone call, fax, or e-mail, no matter how official it may seem.
- Do not respond to e-mail that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the e-mail’s validity using a telephone number or Web address you know to be genuine.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small one. Some thieves hope

small transactions will go unnoticed. Report discrepancies immediately.

- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center. www.ic3.gov
- If you have responded to a fraudulent e-mail, contact the bank immediately so we can protect your account and your identity.
- Ensure that your browser is up to date and security patches applied. Always visit your browser's home page to download the latest security updates even if they don't alert you to do so.