CONNECTIONS
BANK

Internet Security

Your security is important to us. Below are tips 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.”

  - Connections 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 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 573-657-0606.

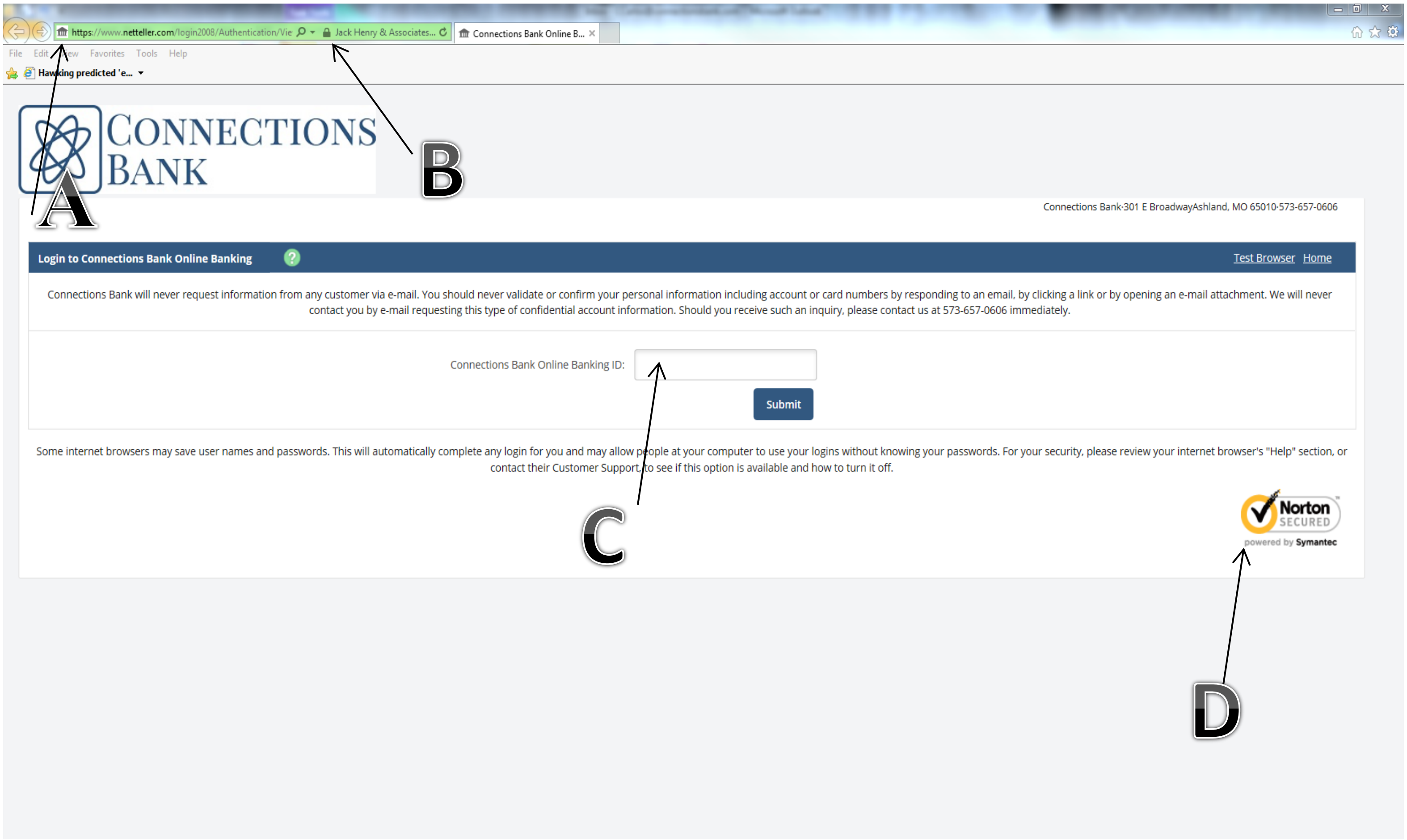
  - Do not complete forms in email messages or reply to an email that ask for personal financial information. Connections Bank will never ask you to reply to or complete such a form within the body of an email message.

- What is “Pharming” or “Spoofing”?

  - “Pharming” refers to the redirection on an individual to an illegitimate Web site through technical means. For example, an online 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.



https://www.netteller.com/login2008/Authentication/Vie
Jack Henry & Associates...
Connections Bank Online B...
File
Edit
View
Favorites
Tools
Help
Hawking predicted 'e...
CONNECTIONS BANK
A
B
C
D
Login to Connections Bank Online Banking
Test Browser
Home
Submit
Norton SECURED
powered by Symantec

Connections Bank·301 E BroadwayAshland, MO 65010·573-657-0606

Connections Bank will never request information from any customer via e-mail. You should never validate or confirm your personal information including account or card numbers by responding to an email, by clicking a link or by opening an e-mail attachment. We will never contact you by e-mail requesting this type of confidential account information. Should you receive such an inquiry, please contact us at 573-657-0606 immediately.

Connections Bank Online Banking ID:

Some internet browsers may save user names and passwords. This will automatically complete any login for you and may allow people at your computer to use your logins without knowing your passwords. For your security, please review your internet browser's "Help" section, or contact their Customer Support, to see if this option is available and how to turn it off.

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. When you see this padlock, it means you are on a site with 128 bit SSL (secured socket layer) encryption.
C. Check your computers settings and turn off *saving usernames and passwords* if this feature is turned on.
D. You can also click here to check the validity of the web site.

- Other Important Security Tips
  - Never give out your 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 an e-mail that may warn the dire consequences unless you validate your information immediately. Contact the company to confirm the e-mails 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 ones. 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 National White Collar Crime Center, at www.ic3.gov.
  - If you have responded to a fraudulent e-mail, contact your 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.