Internet Banking Security Information

About scams and spoofs

Consumer
Alert
» Help protect your accounts
» Beware of fraudulent email
Click for more information

Many financial institutions that do business on the Internet have become the target of fraudulent email and website scams. Every Internet user should know about these spoof (also called **phishing** or hoax) e-mails that appear to be from a well-known company but can put you at risk.

Even if you don't provide what they ask for, simply clicking the link could subject you to background installations of key logging software or viruses.

How to identify online fraud

It is difficult to distinguish if an email is legitimate. Scammers have become increasingly sophisticated in creating fraudulent emails and websites that look authentic. These emails and Websites often appear to be from legitimate companies and include images and logos of these organizations.

Characteristics of fraudulent emails and websites

Our bank will never send out an email requesting you to provide, update or confirm sensitive data.

Spoofs often have a sense of urgency telling clients that if they fail to update, verify or confirm their personal or account information, access to their accounts will be suspended.

Spoof emails typically ask for personal or account information such as:

- Account numbers
- Credit and check card numbers
- Social Security Numbers
- User IDs and passwords
- Mother's maiden name
- Date of birth
- Other sensitive information

They often include links that include a legitimate company's name or website address. The fraudulent emails will disguise or forge the sender's email address so they appear to be from a legitimate company.

How to protect yourself from online fraud

- Never provide personal or financial information to unsolicited email, phone or pop-up website requests.
- Type the Website addresses (URL) into browsers instead of clicking on links in emails.
- Change User IDs and passwords every 30 days.
- Keep anti-virus and anti-spam filtering software on your computer up to date.

If you suspect an email to be a spoof

If you suspect that you've received a fraudulent email, please forward it to us immediately and then delete it from your inbox.

Our e-mail address is: **contact@bankwaverly.com**

For more information on the topic, please read the US-CERT's article, "Recognizing and Avoiding Email Scams" here: https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf

1/14/2020 11:15 PM Citizens State Bank