First County Bank™
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Spear-Phishing and How to Avoid It

The latest twist on phishing is ***spear phishing***. No, it's not a sport, it's a scam in which online scammers masquerade as legitimate businesses and government agencies and target you using personal information that you put on the Internet from your PC or mobile device. Using the information, a ***spear phisher***, posing as a known business, sends you an email that looks authentic and asks you to take urgent action on a familiar matter by clicking a link. A malicious software program is then automatically installed on your computer or mobile device, lying in wait to capture sensitive information.

Some tips that can help you to avoid becoming a victim of spear-phishing:

⇨ **Look for Signs.** When an unsolicited email hits your inbox, check for these signs that the email is actually a spear-phishing attempt:

- ***A suspicious email address.*** The sender's name might be someone you recognize, but the email address may be unfamiliar or strange.
- ***No subject line, or a very vague subject line.*** Spear-phishing emails often use generic subject lines or body text like "found something cool" or "check this out!"
- ***A request for personal information***. Online businesses, including banks, will not ask for personal information, such as usernames and passwords, via e-mail. When in doubt, either call the bank directly or open your computer's Internet browser and type the known website address. Do not use contact information contained in the e-mail, which is likely to be fraudulent.

⇨ **Stop Before You Click on Attachments or Links.** Links and attachments are the keys that hackers use to get viruses into your computer or device. Stop and think before carelessly clicking links.

⇨ **Call and Confirm With the Sender.** Spear-phishing emails often purport to be from trusted businesses. Confirm unexpected emails with links and attachments by contacting the supposed sender via phone or another email account.

⇨ **Keep Your Secrets Secret.** How safe you and your information remain depends in part on you being careful not to post personal information online.

⇨ **Use Passwords That Work.** Every password for every site you visit should be different, include random letters and numbers, and be changed frequently.

⇨ **Keep Patches, Updates, and Security Software Current.** When you get notices from software vendors to update your software, do it. Most operating system and browser updates include security patches. Keep your computer and device internet security, anti-virus software and firewalls updated.

If you have any questions feel free to contact the CustomerFirst Contact Center at (203) 462-4400.