



Is Someone “Phishing” for Your Information?



Internet scammers are casting for people’s financial information by sending emails with hijacked corporate logos on them to deceive consumers into disclosing their bank account information, credit card numbers, passwords, Social Security numbers, and other sensitive personal information.

Unsuspecting victims receive an email asking you to “update,” “validate,” or “confirm” your account information and sometimes they will also threaten to close your account if you fail to respond. The emails will appear to be from legitimate banks, credit card companies or even government agencies. But they are not. This scam is known as “Phishing.”

If a consumer responds to the message and clicks on the link provided it will send you to a website. It will look like a legitimate organization’s website. But it is not. It is a bogus website whose sole purpose is to trick consumers into divulging personal information so the operators can steal your identity.

What can you do to protect yourself?

- **NEVER** use email to send or receive personal or financial information.
- Notify your bank or credit card company of any spam emails.
- Review your monthly bank and credit card statements to check for unauthorized charges.
- Forward spam emails the Federal Trade Commission at spam@uce.gov so that it can be available to law enforcement and for more information on email scam alerts or to file a complaint, visit the Internet Crime Center at www.ic3.gov/.