
FRAUD ALERT!
Financial Fraud UPDATE
ACCOUNT SECURITY
Strategies to Protect Your Identity, Your Accounts and Your Devices
4017

Access to new technology and a variety of internet devices allows each of us the unprecedented ease to visit the online world. The speed and convenience to buy goods; download apps, music and movies; research topics; send messages; and much more is becoming part of daily life. However, there can be a real downside – the ever-present threat posed by cyber-criminals intent on stealing your identity, hijacking your accounts and committing fraud.

Consumer Targeting: A Continuing Threat

Over the past several years, data breach computer attacks have been directed at retailers, healthcare provider systems and insurance companies, among others, for the sole purpose of raiding their proprietary files and stealing their customers' personal information. These cyber-crimes have resulted in millions of records being stolen and then repurposed for criminal use or sold to the highest bidder.

The stolen data is then coupled with the already existing tools of the cyber-criminal trade: targeted phishing, texting, pop-up windows, downloads, and spyware now can contain some bits of personal information. These are the methods designed to trick you into confirming personal financial information and unwittingly revealing your user IDs and passwords.

Fraud Prevention: A Security Partnership

Law enforcement officials have joined with your financial institution to combat these criminals on all fronts. Your financial institution has already made substantial investments in training personnel, upgrading to the latest technology and enhancing security infrastructure with the single goal of protecting your accounts and your personal information. But more teamwork is needed!

Personal diligence is the first line of defense – help safeguard and protect your identity and accounts from theft and fraud by following some basic strategies. Use these precautions in your everyday life, and practice integrated security.

Identity Theft Protection – The Dos and Don'ts

- ☑ Do not reveal any personal information online, unless you are positive about the source and the reason.
- ☑ Don't share your user IDs and passwords with anyone and don't store them on your computer.
- ☑ Do be suspicious of any phone caller asking you to provide financial account or credit card account numbers. Your financial institution will never ask you to verify any personal information – they already have it.

Online Device Protection – A Necessary Step

- ☑ Update your personal anti-virus software regularly on all your devices that allow internet access. Also install anti-spyware and malware protection programs on your computer, laptops, smartphones and tablets.
- ☑ Passwords should be strong and changed regularly. Security experts advise a combination of letters, numbers and symbols.
- ☑ Always sign off and log out properly – follow your financial institution's secured area exit procedures.

Financial Account Protection – Early Detection

- ☑ Review your financial accounts often. If something seems unusual, notify your financial institution immediately.
- ☑ Monitor your credit card accounts closely and report any suspicious activity to your card provider without delay.
- ☑ You are entitled to one free credit report annually from each of the three major credit bureaus. That means you can check for free every four months. Order your Free Credit Report at 1-877-322-8228 or www.annualcreditreport.com

Partner with your financial institution today in the cause of your personal protection!

FAST FACTS ABOUT FINANCIAL FRAUD

- **Data Breach** – An electronic breach of a proprietary file that contains personal information that could potentially lead to identity theft, including Social Security numbers, financial account information, driver's license numbers and medical information.

- **Phishing** – A scam using fraudulent e-mails, appearing to be from a trusted source such as a financial institution or government agency. The e-mail directs you to a fake website that looks legitimate and asks you to "verify" personal information.

- **Government Agency Scams** – The Federal Trade Commission (FTC) reports that cyber-criminals are using phishing scams and telephone calls which ask an individual to update their information. The impostors identify themselves as agents of the Internal Revenue Service (IRS) or Social Security Administration (SSA) and ask you to verify personal information.

  Neither agency initiates contact by telephone, email, text messages or other social media channels to request personal or financial information—period.

  Contact the FTC Consumer Resource Center at **www.ftc.gov** if you believe a scammer has targeted you.

Resources

- Internet Crime Complaint Center
  www.ic3.gov
- Financial Fraud Enforcement Task Force
  www.stopfraud.gov
- Federal Financial Institutions Examination Council Consumer Fraud Center
  https://www.ffiec.gov/cybersecurity.htm
- Federal Trade Commission Consumer Resource Center
  www.ftc.gov
- National Credit Union Administration
  www.ncua.gov
- Federal Deposit Insurance Corporation
  www.fdic.gov