Protecting Your Online Accounts

As financial technology has evolved, it has given consumers the ability to shop, save, and invest online using their phones, tablets, and computers. These modern financial conveniences, however, come with risk. Scammers always look for new ways to get into a consumer's pocketbook, electronically or otherwise. Investors should be cautious in the way they use the conveniences offered by new and evolving financial technology, especially as they've become more widely used during the COVID-19 pandemic. A bit of caution can keep virtual distance between scammers and your money.

Banks, credit unions, brokerage firms, investment advisers, employer retirement plans, personal retirement accounts, and more all offer consumers electronic access to their accounts through websites and mobile apps. Retail investors can make important financial decisions, day or night, from their mobile phones. Not long ago, this sort of ready-access to the financial markets was the realm of science fiction. No longer. Technology allows us to buy securities, send money and pay bills with the swipe of a finger. These conveniences are unfortunately not counterbalanced with comparable protections from fraud or abuse.

Online Accounts, Virtual Shopping, and the Risk to Your Financial Information

The more that financial information is shared through apps, websites, and other digital media, the more it becomes at risk. Scammers can access private information in different ways and use that information to harm your finances. Here are a few examples:

Data Breaches. A data breach is an incident that exposes confidential or protected information, usually involving the loss or theft of private data that can be used by criminals to steal consumers' identities and assets. Data breaches happen to businesses, universities, hospitals, governments, and even credit reporting and monitoring agencies whose job it is to protect such data. Data can be sold or shared with other fraudsters through online black markets that traffic in misappropriated information.

Phishing. Phishing involves scammers using fraudulent emails, text messages, or phone calls to impersonate legitimate people and entities to trick consumers into giving out their personal information. The scammer pretends to be a well-known business, an employer, or some other person or entity the consumer trusts. The scammer then uses a person's presumed trust to request personal data that can be used fraudulently or sold on the online black market.

Skimming. Skimming frauds involve the use of technology fraudulently installed into a debit or credit card reader, frequently at a gas pump or an ATM. When a consumer inserts their card to pay for gas or withdraw money from their account, the skimmer copies or "skims" information from the card, allowing the scammer to make counterfeit versions of the card for fraudulent use.

Public Wi-Fi Scams. Many businesses and public spaces offer free wireless internet for the public to use when going about their daily lives. Unsecured public Wi-Fi is a goldmine for scammers looking to steal personal financial information from people who use these public networks to shop online or access personal information that becomes visible to anyone who wants to see.

These are not the only ways that scammers try to get access to your money, but they are some of the more common ways that bad actors try to use new technology to play old tricks, leaving consumers and investors holding an empty bag.

Issued: Februrary 2021

To learn more, contact the KENTUCKY DEPARTMENT OF FINANCIAL INSTITUTIONS

500 MERO STREET, 2SW19, FRANKFORT, KY 40601 | HTTPS://KFI.KY.GOV | PHONE: 502-573-3390 | FAX 502-573-8787

How to Protect Yourself and Your Financial Information

Monitor Your Accounts. Check your bank, credit card, and brokerage account statements regularly and keep an eye out for fraudulent or suspicious transactions. Contact your bank, credit card issuer, broker, or investment adviser immediately if you see a questionable transaction or charge. Don't hesitate to contact the authorities in cases of fraud. The sooner you dispute a fraudulent or suspicious transaction, the better.

Use Caution on Public Wi-Fi. Public Wi-Fi networks – especially unsecured public networks – carry huge risks. Avoid online shopping and accessing financial or other personal data on public Wi-Fi networks. Wait until you can access an encrypted private network to enter your credit card number or enter account login information.

Check Your Credit Reports. In the U.S., consumers can visit www.annualcreditreport.com at least once per year to check their credit reports from the three major credit reporting agencies for free. In Canada, consumers can visit the federal government's website for similar information. If an entry does not look familiar, consumers should follow up right away. Dispute entries that are fraudulent. Consumers interested in greater peace of mind might consider subscribing to a credit monitoring service.

Be Careful with Debit Cards. Debit cards offer fewer fraud protections than credit cards and leave your bank account vulnerable to scammers who get bank account information or spoof your card. Credit cards offer better fraud protections than debit cards, and consumers should consider using a credit card instead of a debit card anytime they are shopping online or giving a card number to pay for something over the phone.

Speak Up if Something is Wrong. If an investor suspects something is wrong with their account statement or credit report, they should follow up with their financial institution and credit reporting agency to make sure the charge or credit report entry is accurate. Dispute transactions and credit entries that are not legitimate.

The Bottom Line

Be careful when disclosing personal information online and avoid doing it in a public setting at all costs. Use safer methods of payment that come with enhanced fraud protection if possible, and check account statements regularly. Reach out to the Kentucky Department of Financial Institutions before making any investment, or if fraud is suspected.