TREMONT FIRST NATIONAL BANK
TREMONT • HOPEDALE • NEW HOLLAND

You have to experience it!

Cybersecurity Tip of The Week- 9/18/17

Consumers need to be vigilant following the massive Equifax data breach, experts warn. Even if you were wise enough to put an immediate fraud alert or credit freeze on your credit files, con artists are likely to go into hyper drive finding new ways to take advantage of the hack and the publicity surrounding it. Here are three cons that experts believe will become prevalent in the aftermath of the Equifax breach.

Imposter scams

The Federal Trade Commission warned that it expected a new wave of imposter scams, with con artists posing as representatives of Equifax "calling to verify your account information." Given that Equifax is providing free credit monitoring and credit freezes in wake of its data breach, the call may sound legitimate, the agency warned. But don't ever provide any privy information over the phone.

The purpose of this con is to get you to provide private information, including some of the information that was leaked in the breach, to a caller or via email. Even if your information was leaked, not all fraudsters are likely to have access to it.

Providing information to a new con artist over the phone simply increases the chance that you'll be victimized. Of course, if your data wasn't part of the Equifax attack, giving it out over the phone gives you a chance to join your friends and neighbors in having your data exposed on the dark web.

Tax identity theft

The Internal Revenue Service has been fighting tax identity theft for years. These scams involve criminals getting victims' names, addresses and Social Security numbers to file fraudulent tax refund claims. The agency cites data breaches as one of the main ways that con artists get the relevant information to pull off tax identity theft.

Victims often get the first inkling of a problem when they file their annual tax returns and the IRS notifies them that another return has already been filed and their refund has been claimed. While the agency has a task force dedicated to these cons, they are complex and difficult to solve, often taking more than four months to investigate, according to the agency.

If your information was compromised in the data breach, make a point of filing your annual tax return promptly. Take immediate action if you are informed that more than one return was filed in your name, or you owe additional tax, or that IRS records indicate that you earned more than the amount of wage you reported.

What action should you take? File a police report and a fraud report with the FTC Identity Theft Hotline (877-438-4338). Also complete IRS form 14039, the Identity Theft Affidavit. You may be forced to file your tax returns on paper in the meantime. If you do not get a prompt response from the IRS, call the Identity Protection Specialized Unit at 800-908-4490 for assistance.

Spear-Phishing

The data made available through the Equifax breach is also likely to spur a wave of so-called "spear-phishing" scams that could put more than your credit at risk. Phishing scams are often unsophisticated email and phone cons aimed at getting you to reveal privy data, such as your Social Security number. Spear-phishing cons are far more sophisticated.

These use your real data, the type of data compromised in the Equifax breach, to mimic legitimate communication from your bank or broker. The email may urge you to click on a link or open a PDF file to check your account or verify a transaction. However, if you click on the link, you could be downloading malicious software on your computer that would allow the crook to hijack your system or record your keystrokes. The best advice after the Equifax breach is to assume any such communication is suspect. If you get an email from your bank, broker or credit card issuer and believe it's legitimate, visit the company's website, call their toll-free number or talk to an employee you know. ***Do not just click on the link.***