8/16/17

By Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America

The fourth annual " Data Breach Industry Forecast " from Experian Data Breach Resolution paints a scary picture of how identity theft is evolving and the new types of security threats that we are likely to face. Companies, organizations and agencies that hold people's personal information need to be aware of these trends and harden their defenses – and so should consumers.

Watch out for Aftershocks

Did you know that attackers who steal people's user names and passwords in a data breach may continue to sell them to fraudsters for years afterwards? Why would this information still be valuable? Wouldn't the breach victims have changed their user names and passwords? Yes, they probably did, but identity thieves know that people often use the same user names and passwords for multiple accounts and may not bother to change them all when one is compromised. So crooks try to log into accounts on popular financial, retail and social media sites with stolen user names and passwords to see if they work, and sometimes they do. Experian predicts that we'll see an increase in these "aftershock breaches."

Experian recommends that when people are notified about a data breach and instructed to reset their user names and passwords, they should also be informed about the broader risk if they use the same logins for other accounts. It also suggests using two-factor authentication to verify people's identities rather than continuing to rely on user names add passwords. This involves taking an added step like sending a text alert to the person or using something that is unique to them, such as a fingerprint. It could help solve the password and user name reuse problem, but it's still not widely available.

Our suggestions for consumers: Don't use the same user names and passwords for multiple accounts. It's convenient but it's just too dangerous. Ask about two-factor authentication for

your accounts.

Cyber-War may be Looming

There's been a lot of news about cyber-attacks by foreign nations against U.S. interests, from Chinese hackers obtaining the personal information of federal employees from the Office of Management and Budget to Russian hackers stealing emails from U.S. persons and institutions. Experian predicts that state-sponsored cyber-attacks will move from espionage to outright cyber-war, with targeted countries retaliating by launching cyber-attacks of their own. Businesses and individuals will suffer collateral damage if their sensitive information is exposed or the systems they depend on are disrupted.

Experian warns that companies should prepare for "full-on disruption, especially if they are part of the critical infrastructure," and recommends that they take proactive steps such as shoring up their security measures and purchasing the proper insurance protection. Though this report is aimed at businesses, government agencies and nonprofit organizations also need to be vigilant against cyber-attacks, no matter who is behind them.

Our suggestions for consumers: Back everything up. Keep copies of paper documents in clearly labeled files, and keep electronic records on an external hard drive, updating them as needed.

Healthcare Organizations Will Become Big Targets

Personal medical information is one of the most valuable types of data for attackers to steal because they can sell this sensitive information for big bucks on the "dark web." Experian predicts that "mega breaches" will move from insurance companies to other parts of the healthcare industry, such as hospital networks, where it is harder to maintain security measures. Another prime target will be electronic health records. Experian says that the portable nature of this information and the fact that many different entities need access to it means that it is highly vulnerable to theft. While there is generally good security for transmitting electronic health records, it only takes one compromised computer or outdated system to lead to exposure. Mobile applications for electronic health records may introduce new vulnerabilities. In addition, Experian warns that ransomware directed at healthcare system

operations could have a “catastrophic” effect.

Experian recommends that healthcare organizations ensure that they have proper security measures in place and keep them updated, that they have plans for how to respond to a ransomware attack, and that they have adequate employee training about security.

Our suggestions for consumers: Keep your own computers and mobile devices secure to protect yourself from hackers and malware. Follow these easy-to-understand tips for consumers about online security.

Payment-based Attacks Will Continue

The shift to “ chip cards ” to deter counterfeiting credit and debit cards has not put an end to payment breaches. This new technology has been slow to roll out, and while many big name retailers have adopted it, some businesses are having difficulty with making the software updates needed to accept payments with chip cards. Experian predicts that attackers may therefore turn their attention to smaller franchised stores. It also warned that attackers are going to use new techniques to steal payment card information using skimmers. These are often fraudulently placed on gas pumps but Experian warns that their use may grow in places such as self-checkout terminals in stores.

Experian says that it is essential for businesses to implement the chip technology as soon as possible. In the meantime, they should to pay close attention to weak spots to catch skimmers quickly.

Our suggestions for consumers: Your cards may have both a chip and a magnetic stripe. Use the chip feature rather than swiping your card whenever possible to protect your account number from theft.

Another prediction in the report is that companies operating internationally will face new pressures to comply with breach notice requirements that will soon take effect in Europe, Canada and other countries. Experian recommends that they do “dry runs” to ensure that they

have the right practices in place. Other trends to watch include the potential for crooks to target virtual or augmented reality games to steal personal information, and phishing scams focused on employees.

While the threats that Experian forecasts are daunting and there is no way to prevent identity theft 100 percent of the time, the risks can be significantly reduced by following good security practices.