How Consumers Can Protect Their Identity after a Data Breach

Steps to safeguard personal information in a vulnerable cyber-space.

By Paige Schaffer, CEO of Generali Global Assistance's Identity and Digital Protection Services Global Unit

In an age where large retailers, banks, credit bureaus, hospitals, and government agencies keep digital records of sensitive identification information, it's not surprising that sophisticated hackers are targeting these types of institutions to attain personal and financial information. With the steady increase in both the size and frequency of data breaches, it's easy for individuals to feel powerless against faceless criminal hackers. This feeling is exacerbated by the fact that these cybercriminals are evolving, becoming more advanced as they continue to lay siege against the latest in cybersecurity technology.

While hackers and identity thieves become more sophisticated and resourceful, consumers remain stagnant in their efforts to safeguard their identity. According to Generali Global Assistance's 2019 Global Cyber Barometer Survey, 45% of people reported they wouldn't know what to do if their information was compromised in a data breach.

With each breach, consumer education plays a vital role in protecting personal identification information because these cyber-attacks are becoming more targeted and increasingly successful in attaining the most sensitive of personal information. The question becomes: how can we, as consumers, safeguard our personal information post-data breach?

Get all the information

Immediately following disclosure of a data breach, affected consumers need to learn as much as they can about the attack, including when the breach occurred and what information was stolen. After learning what data was stolen, it's important to determine the level of risk associated with the stolen information.

The most sensitive piece of information hackers can steal is a person's Social Security Number (SSN), because it's a life-long form of identification that cannot simply be canceled. Although a new SSN can be issued in extreme circumstances, this doesn't always guarantee a fresh start; often, the old SSN will still be linked to the victim – often cropping up as sub-files on their credit profile, continuing to cause harm. Since SSNs are required when applying for lines of credit, purchasing a home, or securing additional government documents, it's the gift that keeps on giving for criminals. Victims who have their SSN stolen will have an elevated risk of identity theft for life.

Driver's licenses, usernames, credit cards, and passwords are much less damaging than a stolen SSN because these items can easily be changed and/or replaced. Though this information falls into a lower-risk tier than SSNs, consumers should still exercise caution, as hackers can leverage this stolen data to solicit additional personal information from individuals affected by such a data breach.

Take action

After learning what data was taken, affected individuals should immediately change the stolen information such as usernames, passwords, and security questions from the breached account. It's best to change login credentials regularly, given that institutions are not required to disclose hacks right away. This often provides thieves with enough time to sell login information on the dark web before the data breach is announced.

When creating a new password or changing an existing one, it's important to use strong, unique passwords and to never reuse passwords across multiple platforms. Reusing the same password creates a "skeleton key" for hackers, providing them with access to multiple accounts rather than just the one account that was exposed.

In the event that credit card or other sensitive banking information was compromised, it's imperative to contact the associated financial institution, cancel all affected cards and request replacements for each canceled card. For consumers who prefer to be on the safer side, it would be prudent to initiate a credit freeze, which is available to all consumers at no cost. Credit freezes restrict access to an individual's credit report and make it difficult to open new accounts under their name.

After completing these steps, consumers should remember to update automatic bill withdrawals with the new credit card information and lift the credit freeze if they plan to apply for a line of credit.

Stay vigilant

Mitigating fraudulent activity begins with monitoring for suspicious activity on credit reports and any financial accounts. Consumers should set frequent, recurring reminders to search for any unauthorized movement on statements, credit reports, and other financial documents – particularly after a breach. Oftentimes, identity thieves will patiently wait until the breach is considered "old news" before using the stolen information to their advantage.

Because cybercriminals have extended patience, affected individuals should be very wary of unexpected emails years after the cyberattack. Once thieves have access to consumers' contact information, they can use the data to create highly-targeted and personalized phishing emails, providing them with additional opportunities to solicit more personal information from victims.

Breach victims should be cautious of emails from banks or other institutions that request personal information, uncharacteristic requests from colleagues or family members, and emails that aggressively direct readers to click a link (i.e., "OMG, did you see this crazy video?").

Be proactive

Even when consumers take these actions post-breach, there's no guarantee that it will stop cybercriminals in their tracks. That's why being proactive about identity protection is crucial in this digital age.

According to Generali Global Assistance's consumer research, 79% of individuals classify identity theft as a top concern, ranking it above serious illness and injury, car accidents, and home robbery. Having a proactive identity protection plan in place will reduce the panic and stress that accompanies future breaches.

In this digital age, it's important for consumers to consider the personal information they share online. With all the data leaked in cyberattacks, hackers can piece together a holistic picture of an individual's identity by combining stolen information with details that are publicly shared online such as birthdays, addresses, employers, etc.

In conjunction with the previously suggested measures, consumers would be wise to invest in identity protection services that can help manage many of these safeguards a lot more easily via credit and identity monitoring, as well as online data protection tools that can help keep hackers at bay on personal computers.

When assessing identity protection services, individuals should look for providers who offer comprehensive services that include essential features like continuous automated and human surveillance on the dark web and black market for personal identification information, round-the-clock access to an identity theft support center, and identity theft insurance to cover the costs associated with restoring a consumer's identity, should they become victims of identity theft or fraud.

With the increasing frequency of data breaches, the number of exposed sensitive records has increased 126% year over year, according to the ITRC's 2018 data breach report. This means that the occurrence

of identity fraud for consumers is just a matter of timing. With these combined measures and precautions, consumers have the power to fight back against faceless cybercriminals and reduce their risk of identity theft – not just after the next massive data breach, but before it ever happens.

About the Author

Paige Schaffer is CEO of the Identity and Digital Protection Services Global Unit for Generali Global Assistance. Ms. Schaffer leads sales & marketing strategy and revenue growth initiatives, managing operations as well as global expansion. Schaffer began her tenure with Generali Global Assistance in 2007 and led North America Operations for both the emergent Travel Assistance business and the Medical Claims division, working with insurers, medical providers, and government contractors. Ms. Schaffer is a thought leader on identity theft protection, resolution, and victimization. For more information, visit https://us.generaliglobalassistance.com/.