JTD
Financial Services, LLC

167 South River Road ◇ Suite 11 ◇ Bedford, NH 03110
www.jtdfinancial.com

Data Breach: Your Security To-Do List

According to recent statistics, data breaches have become common in today's digital world. In fact, it is estimated that more than 111.7 million Americans have their personal information exposed to data breaches every year. Whether it's a major retailer, a subscription service, or another online platform, the risk of a data breach is a reality that we all face.[1]

Names, email addresses, passwords, and other sensitive information are being swept up by hackers for fraudulent activities. These breaches come in two flavors: breaches of institutions that people trust with their data, such as retailers and banks, and breaches of entities that acquire user data secondarily, such as credit bureaus and marketing firms. However, individuals can take steps to protect themselves and minimize the impact of a breach.

If you receive a notification that your sensitive information has been stolen in a data breach, it's important to take immediate action to mitigate the damage. Data breaches can occur even if you practice good cybersecurity habits and are not personally targeted. Organizations and businesses can leak data due to human error, leaving your information vulnerable to bad actors.[2,3]

To help you navigate this stressful situation, we have compiled a checklist of steps you should take if you have experienced a data breach.

1. **Stay informed:** Keep yourself updated about the breach by setting up news alerts or signing up for updates from the affected company. This will ensure that you are aware of any developments or actions being taken to address the breach.
2. **Understand what data has been compromised:** Read the notification carefully to understand what specific information may have been exposed.

This could include your name, address, email, passwords, credit card details, or even your Social Security number. Knowing exactly what data has been compromised will help you take appropriate action.

3. **Set up multi-factor authentication:** Enable multi-factor authentication for all your online accounts. This adds an extra layer of security by requiring a second form of verification beyond your password, such as a unique code sent to your phone.
4. **Change passwords:** Change the passwords of all your online accounts, especially those that may have been compromised. Use strong, unique passwords for each account, and consider using a password manager to keep track of them.
5. **Credit and financial accounts:** Monitor your credit reports and financial accounts for any suspicious activity. You can request a free credit report annually from each of the three major credit bureaus (Equifax, Experian, and TransUnion.)
6. **Watch out for phishing attacks:** Be vigilant against phishing attempts, in which scammers try to trick you into revealing personal information or login credentials. Be skeptical of emails, messages, or phone calls asking for personal information or directing you to click suspicious links, and avoid clicking those links or providing sensitive information through email or phone calls. When in doubt, contact the organization directly through its official website or phone number to verify the request.
7. **Report identity theft:** If you suspect you are a victim of identity theft, report it immediately to the Federal Trade Commission (FTC) through its website IdentityTheft.gov. This resource will guide you through the necessary steps to recover from identity theft and protect yourself from further harm.
8. **Use strong, unique passwords:** Avoid using common or easily guessable passwords. Instead, use a combination of letters, numbers, and symbols. Additionally, use a different password for each online account to minimize the risk of multiple accounts being compromised if one password is breached.
9. **Be cautious of phishing attempts:** Phishing is a common tactic used by hackers to trick individuals into revealing their personal information. Be skeptical of emails, messages, or phone calls asking for personal information or directing you to click on suspicious links. When in doubt, contact the organization directly through their official website or phone number to verify the request.
10. **Update your software:** Keep your operating system, web browser, and antivirus software up to date to ensure you have the latest security patches and protections against known vulnerabilities.
11. **Limit the information you share:** Be cautious about sharing personal information online, especially on social media platforms. Avoid posting your full address, phone number, or other sensitive details that could be used for identity theft.
12. **Use secure Wi-Fi networks:** When accessing the internet in public places, use secure, password-protected Wi-Fi networks. Avoid using public Wi-Fi networks that are unsecured, as they can easily be intercepted by hackers.

13. **Regularly back up your data:** To be prepared for a breach or other data loss event, regularly back up your important files and data to an external hard drive or cloud storage service.

While these steps can minimize the risk of personal data breaches, it's important to remember that no security measure is foolproof. It's crucial to stay vigilant and be proactive in protecting your personal information.[2,3]

Experiencing a data breach can be a stressful and overwhelming situation. Following this checklist enables you to take the necessary steps to protect yourself and minimize the potential damage caused by the breach. Remember to stay informed, be proactive in securing your accounts, and report any suspicious activity to the appropriate authorities.

[1.] Zippia.com, June 15, 2023
[2.] Wired.com, February 17, 2023
[3.] FultonBank.com, July 27, 2023