Tips on Recovering from a Data Breach and Successfully Weathering the Digital Storm

With the recent increases in data breaches, there are several important actions that you can take to protect yourself and recover from personal data loss or compromised credit cards. Texas A&M Engineering Extension Service (TEEX) cybersecurity experts have developed these tips to help individuals recover from a data breach and successfully weather the digital storm.

- **Read up on the data breach** – knowing what kind of sensitive data was impacted can help steer your next steps.
- **Check your financial accounts and credit score** – keep close tabs on your bank account, your credit card usage, and accounts handling your investments. Fraudulent charges to your credit card may be disputed and possibly reversed. A credit monitoring service can immediately inform you if someone has stolen your identity.
- **Freeze your credit** – one of the most damaging outcomes of a data breach is identity theft and the resulting destruction of your credit score. Learn how to freeze your credit at each of the three major credit reporting agencies. It's quick and easy! Visit https://www.usa.gov/credit-freeze to learn more.
- **Accept the offer of help from the organization that lost your data** – the company that lost your data may offer some form of compensation, usually in the form of one- to three-years of free credit monitoring.
- **Start using a password manager and change your passwords** – it is correct to assume that your password to a website or account that has been breached should no longer be used. This is a good time to purchase and set up a premium password manager. A password manager is a technology tool that helps internet users create, save, manage and use passwords across different online services. There are several of these out in the marketplace. Have your password manager help you reset all your passwords to your online accounts.
- **Use your password manager to create fake answers to your security questions** – resetting your password will be undermined if the cybercriminals also obtained access to the answers to your security questions on your accounts, such as your mother's maiden name or the make and model of your first vehicle. If you use the same answers to security questions on multiple accounts, those answers will need to be updated. Use your password manager to set them to a random password to thwart cybercriminals.
- **Set up two-factor authentication on all your accounts** – this is especially important for your primary email account, where all your other accounts would send password reset emails. Two-factor authentication is an identity and access management security method that requires two forms of identification to access resources and data. Two-factor authentication applications, such as Duo, or a physical USB security key, are most effective in protecting your data.
- **Check out IdentityTheft.gov if someone has used your information to impersonate you** – This website has personalized recovery plans to help you take back control of your personal information with pre-filled forms, progress tracking and more.

For more information about how TEEX can help you and your organization protect your sensitive data, contact one of our cybersecurity experts at cyberready@teex.tamu.edu.