Protecting Yourself from Cybercriminals

The Staggering Growth of Cybercrime

Cybercrime is a rapidly growing and increasingly costly problem globally. The annual monetary damage from cybercrime reported by the American public is staggering and continues to rise dramatically:

Year	Complaints (#)	Losses ($)
2023	**880,418**	**12.5B**
2021	847,376	6.9B
2019	467,361	3.5B

The global impact to individuals, businesses, and governments is projected at an astounding $11 trillion in 2023, and is expected to grow to $20 trillion by 2026.

The Dark Web

What is it? The dark web is a part of the internet that is not indexed by search engines and can only be accessed using specialized software, such as the Tor browser. This specialized browser grants users a level of anonymity that is especially appealing to cybercriminals, hackers, and government operatives who want to hide their identity.

Is my personal information on the dark web? Avoid searching the dark web directly since it is complex and difficult to navigate without specialized tools and knowledge, and may result in downloading files or clicking links that can expose you to malware and viruses. Instead, use free dark web scanners from reputable sources, such as Experian, to check if your personal information has been compromised.

Proactively Protecting Your Online Personal Data

Protecting your personal data is crucial in today's digital age. Here are 10 essential steps you can take:

1. **Create strong passwords**: Use a combination of upper and lowercase letters, numbers, and symbols. Consider using a password manager to generate and store complex passwords securely.
2. **Enable Two-Factor Authentication (2FA)**: This adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone.
3. **Beware of phishing attempts**: Be cautious of suspicious emails, links, or calls that ask for personal information.
4. **Secure your devices and keep software updated**: Use strong passwords, encryption, and antivirus software on your computers, smartphones, and tablets and regularly update your operating system, apps, and antivirus software to patch vulnerabilities.
5. **Limit personal information sharing:** Be mindful of the information you share online, including on social media platforms, and over the phone.
6. **Be cautious with public Wi-Fi**: Avoid accessing sensitive information on public Wi-Fi networks. Use a VPN for added protection.
7. **Backup data**: Create regular backups of your important data to protect against data loss.
8. **Be careful with online shopping**: Use secure websites (those with "https" in the URL) and avoid sharing personal information unnecessarily.
9. **Monitor your credit profile and sensitive personal information online**: Regularly check your credit report and financial accounts for any suspicious activity.
10. **Use automated monitoring services**: Sign up for 24/7 credit monitoring and enroll in ID theft protection.

Protecting Yourself from Cybercriminals

Steps to Take If Your Personal Data Has Been Compromised

Discovering that your personal data has been compromised can be alarming, but taking action quickly (within first 48 hours) can help mitigate the damage. Here's a step-by-step guide:

- ❑ **Change passwords immediately:** Update passwords for all online accounts, especially those using the compromised email or password.
- ❑ **Enable two-factor authentication**: Activate 2FA wherever possible for an extra layer of security.
- ❑ **Monitor financial accounts**: Keep a close eye on bank, credit card, and other financial accounts for unusual activity.
- ❑ **Contact financial institutions**: Inform your banks and credit card companies of the data breach and request fraud alerts or temporary account freezes.
- ❑ **Order credit reports**: Obtain free credit reports from all three major credit bureaus (Equifax, Experian, and TransUnion) to check for suspicious activity.
- ❑ **Create fraud alerts**: Inform credit card companies and other potential lenders that you may be a victim of fraud or identity theft by placing a fraud alert with credit bureaus.
- ❑ **Place a credit freeze**: Consider placing a credit freeze on your credit report, making it difficult for anyone to open new accounts in your name.
- ❑ **Consider identity theft protection**: Enroll in an identity theft protection service for added monitoring and support.
- ❑ **Be wary of phishing attempts**: Be cautious of emails, calls, or texts requesting personal information, as these could be attempts to exploit the situation.
- ❑ **Review online accounts**: Check privacy settings on social media and other online accounts to ensure personal information is protected.
- ❑ **Report the breach**: If applicable, report the data breach to the appropriate authorities, such as the FTC, FBI, your State Attorney General's Office, and local police.

Credit and Identity Theft Protection Services

Many companies offer free credit and identity theft protection services:

- **Credit Card Companies**: Some credit card companies offer free credit monitoring and ID theft protection as a perk to their cardholders.
- **Banks and Credit Unions**: Many financial institutions provide basic fraud alerts and monitoring services to their customers at no charge.
- **Credit Bureaus**: All three major credit bureaus offer free credit reports weekly through **AnnualCreditReport.com,** and some offer credit scores and monitoring services for free. Regularly reviewing your free credit reports can help you identify potential issues.
- **Credit Karma**: Provides free credit scores and reports from Equifax and TransUnion, along with some basic monitoring features.
- **Other sources**: You may also have a free identity theft protection plan through your employer, and some renters and homeowners insurance policies may include protection for financial accounts.

Also, if you're affected by a data breach, you'll likely be offered free credit or identity theft monitoring for a time. Consider paying for a service only if you're already the victim of identity theft or at high risk of it, are unwilling to freeze your credit and won't monitor your own data.

DIYMONEYTRACK.com