Identity Theft & The Dark Web

What do Minneapolis High Schools, T-Mobile, Norton Life Lock, Uber, LastPass, PayPal, and Twitter all have in common? They've all suffered from massive hacks in 2023. After most data breaches, the stolen data is sold on the dark web making thousands to millions of dollars for the person stealing the data.

What is Identity Theft

Identity theft is when thieves use someone's personal data to take over or open new accounts for financial gain. Personal data includes name, date of birth, Social Security number, account ID, email, bank account, credit card number, PIN numbers, password, address, phone, or lots of other information. Your personal data is always at risk and can be stolen long before you realize you're a victim.

Ways Your Identity is Stolen:	Ways Your Identity is Used by Thieves:
1. Data Breaches (Most Common) 2. Malware and Spyware Activity 3. Scams, Phishing, and Spam Attacks 4. WiFi Hacking (Very Rare)	1. Open fraudulent credit card accounts in your name. 2. Use your credit cards or account numbers to make purchases. 3. Sell your personal information on the Dark Web. 4. File fraudulent taxes and/or steal your tax refunds. 5. Use your ID and password to access financial accounts.

What is the Dark Web

The Dark Web is NOT a site at: WWW.DarkWeb.Com. The Internet is made up of the Surface or Clear, Deep, and Dark Webs. The “Surface or Clear" web is 4% of the Internet that can be accessed without a password from any browser and is regularly indexed by search engines like Google and Bing. The "Deep" web is 90% of the Internet, that is the unindexed Internet that requires passwords. The deep web contains mostly benign sites, such as your password-protected email account, paid subscription services, Medical records, company private websites, and others. The "Dark" web is 6% of the Internet used for illegal activity like illegal drugs, weaponry, stolen personal data dumps, counterfeit money, and websites or forums which host illegal content like child pornography or white supremacy.

The Dark web requires specific software, configurations, and authorization to access. Dark websites are accessible only through networks such as Tor “anonymity network” and I2P “Invisible Internet Project”. Tor focuses on providing anonymous access to the Internet, I2P specializes in allowing anonymous hosting of websites. Identities and locations of Dark web users stay anonymous and cannot be tracked due to the layered encryption system.

Dark Web sites increase the value of the stolen private data by aggregating it with other publicly available data. An individual’s data can cost anywhere from pennies to up to $300. The buyers of this info are spammers and credential stuffers who take usernames and passwords leaked from one site to log into accounts on other websites where the users have used the same credentials. Video 3:53: https://www.cnet.com/videos/finding-our-personal-data-on-the-dark-web-was-far-too-easy/

Tips to Protect Yourself

- Almost everyone has had data stolen. Use “Have I been Pwned” https://haveibeenpwned.com/ to check for data breaches involving your email. Over 12 billion accounts have been breached and are for sale.
- #1, #2, #3 Create strong passwords unique to each of your online accounts, change them routinely and never reuse old ones. Use the free secure password manager like Bitwarden https://bitwarden.com. See the April 2022 Learn About – Online Security & Passwords for more detail. I don’t recommend using the password managers that come with most browsers due to the lack of features. Some apps or sites let you use your GMail or Facebook account to login, and always create a new account with a different password.
- If you hear of a breach, change your password immediately! It can be as little as several days or even ten years later where your data will be used.
- Enable two-factor authentication “2FA” where you will use a secondary form of authentication, often a Text message sent to your phone or authentication app. A stolen password is useless without that additional factor. Especially important on financial, banking, and email sites. eMail because that is the way most sites let you reset a password.
- Watch your credit card and bank statements for unexpected charges and payments. Turn on notifications from your bank, brokerage, and Credit cards of transactions. The free online service Mint lets you monitor your finances in one place instead of multiple logons.
- Go paperless when you can. Statements are securely delivered to and stored right in your account online.
- If you choose not to create an online account you are more vulnerable than if you do create an account. Online services like a bank make it easy to setup a new online account using limited personal information.
- Lock up sensitive documents and always shred or use a certified document destruction service to destroy them.
- Never give your personal information to someone who calls, emails, or texts you if you did not initiate the request.

- Don't respond to or click links in a text, email or social media post from someone claiming to be from a government agency, known company, or bank if you didn't initiate the request.
- You can request one free credit report a year from the three credit services: Equifax, Experian and TransUnion at: https://www.annualcreditreport.com Look for unusual activity, such as the appearance of new accounts. Space out the three requests so you check every four months from a different service.
- Freeze your credit for free to stop anyone from opening credit and requesting loans and services in your name. You can unfreeze your credit as needed.
  - Experian: https://www.experian.com/freeze/center.html
  - Equifax: https://www.equifax.com/personal/credit-report-services/credit-freeze/
  - TransUnion: https://www.transunion.com/credit-freeze
  - Beware of fake websites, emails, or phone calls from scammers posing as one of the three services.
- Sign up for a credit monitoring service. Pick a credit monitoring service that constantly monitors your credit report on major credit bureaus and alerts when it detects unusual activity. To help with the monitoring, you can set fraud alerts that notify you if someone is trying to use your identity to create credit. A credit-reporting service like LifeLock can cost $10 to $30 a month or you could use a free service like the one from Credit Karma. https://www.cnet.com/news/best-identity-monitoring-services/
- Use a mobile-based payment system like Apple Pay or Android Pay. They are more secure than using physical credit card numbers that might be stolen. PayPal should also be used where possible instead of your credit card number.
- A virtual private network "VPN" can help protect your privacy especially when you're on a public Wi-Fi. I do not see a need other than a public Wi-Fi connection and the overhead and problems it can cause is not worth the trouble for other connections.
- Be cautious in downloading browser extensions, and delete ones they no longer need. Eight widely used browser extensions have been caught harvesting data from an estimated 4 million consumers who use the browsers Chrome and Firefox. The extensions collected a host of information that wasn't authorized by either browser, exposing not only complete browsing histories but also access to files such as tax returns, medical records, credit card information, and other highly sensitive data. All the extensions have been remotely removed from or disabled in consumers' browsers and are no longer available for download, but hackers are always working on new attacks with new extensions.
- Use a different eMail addresses for different kinds of accounts. Consider maintaining one email address dedicated to signing up for apps that you want to try, but which might have questionable security, or which might spam you with promotional messages. After you've vetted a service or app, sign up using one of your permanent email accounts. Many sites equate your email address with your username, but some let you select your own username. Consider using a different username every time. Your password manager remembers it, so you do not have to.
- Keep your Operating System "OS" and Apps updated. Delete Apps you do not use.
- On social media sites like Facebook use the built in security to limit what personal information you make public.
- Don't pay for identity theft insurance. Banks cover most losses and 90% of victims have no out of pocket loss.
- See the Nov 2021 Past Carondelet handout/video on Scams & Cyber Threats.
- See the April 2019 Past PCC handout on "Viruses & Security" for many tips. Make sure to have your Anti-Virus installed, updated, and configured correctly.
- As soon as you suspect your ID has been stolen you can take action to stop unauthorized charges and start to recover your identity.
  - Place a fraud alert with each of the credit reporting companies: Equifax, Experian and TransUnion. The alert notifies creditors that you have been a victim of fraud and lets them know to verify that you are actually making new credit requests in your name. You can place an initial fraud alert, which stays on your credit report for 90 days, or an extended fraud alert, which stays on your credit report for seven years. Placing a fraud alert does not affect your credit score.
  - Contact fraud departments for each business and credit card company where you think an account was opened or charged without your knowledge. While you are not responsible for fraudulent charges to an account, you need to report the suspicious activity promptly.
  - Document everything by keeping copies of all documents and expenses and records of your conversations about the theft.
- Create a recovery plan. The Federal Trade Commission has a valuable tool that helps you report identity theft and recover your identity through a personal recovery plan. If you think you are a victim of identity theft immediately submit a report about the theft to the Federal Trade Commission's website: https://www.identitytheft.gov and you will receive a plan.

Additional Links and Information

Carondelet Tech Help Resources: https://carondeletvillage.org/tech-help-resources/
Questions or comments can be sent to: TCKreuzer@gmail.com