Identity Theft & The Dark Web

Last month background check provider National Public Data “NPD” was in the news for a data breach of almost 3 billion names, email addresses, phone numbers, Social Security numbers, and address history (three decades' worth). NPD makes money by collecting and selling access to your personal data to credit card companies, employers, and private investigators. The Social Security number and address history makes it possible for identity theft schemes, such as fraudulently obtaining a bank loan, opening a credit card, or filing IRS tax refunds. This breach is on top of the thousands of other breaches over the years like American Express, 23andMe, Equifax, LinkedIn, T-Mobile, Xfinity and many other businesses. After every data breach, the stolen data is sold on the dark web making thousands to millions of dollars for the person or group stealing the data. We all are at risk.

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 are told or 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	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.

Tips to Protect Yourself

Everyone has had data stolen even if you have never had a computer or smartphone. Use https://HaveIBeenPwned.com/ to check for data breaches involving your email. Over 14 billion accounts have been breached and are for sale. Most of the NPD breach data does not have an email so use https://npd.pentester.com/ or https://npdbreach.com/ to check if your Social Security number is exposed. Our data is out there in the Dark Web and we all need to protect ourselves.

- Freeze your and your kids credit for free to stop thieves from opening accounts, loans, and services using your stolen identity. You must freeze it at all three below and 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.
- You can request one free credit report a year from each of 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.
- Don't waste your money on Identity Theft Monitoring Services or Insurance like LifeLock or McAfee+. They charge up to $40 a month, but taking the tips here you can do a better job for free. The services or insurance hype fear tactics and make fake claims on how they can help. They will report your info is on the Dark Web, but there's nothing it can do to remove it and will repeat the tips I list. Many services brag about covering your losses up to one million dollars. Almost all identity theft victims get their money back without any insurance.
- Create strong passwords unique to each of your online accounts, change them routinely and never reuse old passwords. I highly recommend everyone use the free password manager https://Bitwarden.com. 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 password will be used. Use a passkey instead of a password on sites and services that support passkeys. See the past February 2024 "Online Security & Passwords" presentation for more detail.
- 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 is important because it 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.
- 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 set up 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.
- 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.
- Keep your Operating System "OS", Apps, and Antivirus 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.
- Resources available at the Social Security Administration: https://www.ssa.gov/fraud/
- 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 free 1 year fraud alert at https://www.experian.com/fraud/ or call 1-888-397-3742. The alert notifies all three credit services that you have been a victim of fraud so extra security and monitoring will be done.
    - Contact fraud departments for each credit card company and business 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 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 follow the 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