ID Theft Probability Score For Minors

Answer Key

1. What would happen if you and your friend have a fight? If they know your passwords, you may be setting yourself up for some sort of retaliation. Remember 'revenge is sweet'. Don't set yourself up to be cyberbullied or scammed. Here's why you shouldn't share your passwords.

2. The problem with using the same password on all your accounts is that if a scammer gets access to one of your accounts, they will have access to all your accounts. And possibly to your family's information as well.

3. Scammers are professionals and good at what they do. Many scams target children and teens and tempt you with emails promoting scholarship help, great deals with online shopping, or offers for big money by work-from-home jobs. Some scams are designed to get your money; some just put malware on your devices. Educate yourself and your family so you can take precautions to prevent fraud.

4. People younger than 20 had the biggest year-over-year increase in fraud reports between 2019 and 2020.

5. You've probably already heard many people talk about the risks of public WiFi, but what's the harm in reading one more article to ensure you know all the pitfalls. Risks of Using Unsecured WiFi.

6. Children can be vulnerable targets for identity theft, because those under the age of 18 typically do not have credit reports. That means children are often a blank slate for fraudsters who can apply for credit and take out loans in their name. Identity theft affects 1.25 million kids — or about one out of 50 children — every year, according to the research firm Javelin. Kids usually don't find out they've been victims of identity theft until they take a big life step like applying for federal student aid or buying their first car. Go to www.annualcreditreport.com to see if you have a credit report.

7. Read about protecting your Social Security number from identity theft here.

8. Watch the video on this site to learn about 2-factor authentication

9. Fake game apps often promise exclusive freebies and content, but, in reality, these apps may harvest users' personal and financial information or install malicious software on victims' devices. Learn to spot online gaming scams here and here and here.

10. If you decide to use a peer-to-peer program, use your security software to scan any files before you open them and before you play any downloaded files. Avoid any peer-to-peer program that asks you to disable or change the settings of your firewall. Disabling or changing these settings could weaken your computer's security.

11. Lock down your privacy settings including location on all social media, here's why.

*The more points you get, the more likely you are to become a victim of id theft or scams.

November 2022