What is Financial Identity Theft Prevention?

Worksheet

Financial identity theft prevention is the practice of safeguarding personal data through monitoring, strong security practices, and proactive fraud alerts.

Questions

1. A thief uses your SSN to open credit cards. This is called…

A) Account takeover
B) Financial identity theft
C) Phishing
D) Hacking

2. Which protection stops new accounts from being opened in your name?

A) Fraud alert (7 years)
B) Credit freeze
C) Password manager
D) 2FA

3. True or false: You should use the same strong password for all accounts.

A) True
B) False

4. Which is the safest way to log into your bank if you received a phishing email?

A) Click the link in the email
B) Type the bank's URL directly
C) Use a saved browser bookmark
D) Call the bank first

5. You find an unknown bank account opened in your name. What should you do?

6. Your email was hacked. How do you protect your financial accounts?

7. You receive a phishing email claiming to be your bank. What's safe to do?

8. Define: What is financial identity theft?

9. Define: What's a credit freeze?

10. Define: How often should you check your credit report?

Answer Key

1. B) Financial identity theft — Using someone's personal data to commit fraud is identity theft.

2. B) Credit freeze — A credit freeze prevents lenders from accessing your credit, blocking new account openings.

3. B) False — False — use unique passwords everywhere. One breach compromises only that account.

4. B) Type the bank's URL directly — Always navigate directly by typing the URL, never via a link in email.

5. 1. Contact the bank and report the fraudulent account. 2. File an identity theft report with the FTC (IdentityTheft.gov). 3. Place a fraud alert on your credit file (7 years). 4. Freeze your credit with all three bureaus (Equifax, Experian, TransUnion). 5. Monitor credit reports quarterly for further fraud.

6. 1. Change email password immediately (strong, unique). 2. Enable 2FA on email and all linked financial accounts. 3. Check password manager for compromised passwords. 4. Review account recovery options (phone, backup email). 5. Run credit and bank account scans for unauthorized access.

7. 1. Do NOT click links or download attachments. 2. Go directly to your bank's website (type URL, don't use email link). 3. Log in and check for alerts or unauthorized activity. 4. Report the phishing email to your bank and to anti-phishing authorities (phishing@apwg.org).

8. Criminal use of your personal data (name, SSN, credit card) to commit fraud, open accounts, or take out loans.

9. Locks your credit so no one (including you) can open new accounts without unfreezing. Costs 0–3 per bureau.

10. At least annually (free at annualcreditreport.com). Check more often if at risk or after suspicious activity.