Identity Theft

Multiple-Choice Quiz

1. What is identity theft?
A) Using someone else's personal information without permission for financial gain
B) Stealing physical objects from someone's house
C) Copying someone's homework
D) Pretending to be someone on social media for fun

2. Which of the following is a common type of identity theft?
A) Medical identity theft
B) Academic identity theft
C) Property identity theft
D) Fashion identity theft

3. Which of these personal details is most valuable to identity thieves?
A) Favorite color
B) Social Security number
C) Shoe size
D) Hobby

4. What is "phishing"?
A) A type of fishing using social media
B) A scam where attackers pretend to be trusted entities to steal personal information
C) Sending promotional emails from a company
D) Catching fish in lakes illegally

5. Which of these is a warning sign of identity theft?
A) Receiving bills for unknown accounts
B) Forgetting your own password
C) Losing your wallet temporarily
D) Getting spam emails

6. What should you do immediately if you suspect identity theft?
A) Ignore it
B) Change your passwords and notify financial institutions
C) Post about it on social media
D) Wait for it to resolve itself

7. What is "account takeover"?
A) Hacking into someone's social media for fun
B) Using someone else's personal data to gain access to their accounts
C) Merging two bank accounts

D) Taking a new account at a bank

8. Which government agency in the U.S. helps victims of identity theft?
A) FBI
B) FTC (Federal Trade Commission)
C) CIA
D) NSA

9. What is a “credit freeze”?
A) Temporarily stopping spending
B) Restricting access to your credit report to prevent new accounts from being opened
C) Closing all credit cards permanently
D) Freezing cash in your bank account

10. Which of the following is safest for online shopping?
A) Using public Wi-Fi without a VPN
B) Using secure, HTTPS-enabled websites
C) Entering your Social Security number on any website
D) Sharing passwords with friends

11. How can identity thieves obtain your personal information?
A) Dumpster diving
B) Hacking computers
C) Skimming credit/debit cards
D) All of the above

12. What is “synthetic identity theft”?
A) Using fake identities made from real and fake information
B) Stealing only synthetic products
C) Hacking social media bots
D) Pretending to be a famous celebrity

13. Which of these is a preventative measure against identity theft?
A) Sharing your passwords with friends
B) Shredding documents containing personal info
C) Using the same password everywhere
D) Clicking on random email links

14. Which is NOT a common target of identity thieves?
A) Bank account numbers
B) Social Security numbers
C) Pet’s favorite toy
D) Credit card numbers

15. How often should you check your credit report to detect fraud?

A) Once every 10 years
B) Annually or more frequently if you suspect fraud
C) Never
D) Once in your lifetime

16. What is “shoulder surfing”?
A) Watching someone’s shoulder movements
B) Observing someone to steal sensitive information like PINs
C) Playing a surfing video game
D) Looking at fashion trends

17. Which type of identity theft involves using someone else’s personal info for tax fraud?
A) Financial identity theft
B) Tax identity theft
C) Medical identity theft
D) Social media theft

18. What is the first step in recovering from identity theft?
A) Filing a police report
B) Ignoring it
C) Selling personal data
D) Closing your social media accounts permanently

19. What does “skimming” refer to in identity theft?
A) Quickly reading emails
B) Stealing card information through a small device on ATMs or point-of-sale systems
C) Using skim milk
D) Skipping through bank statements

20. Which of these passwords is safest?
A) 123456
B) Password
C) Th!$1s@C0mpl3xP@ss
D) MyName123

21. What is “social engineering” in identity theft?
A) Building social media networks
B) Manipulating people to reveal confidential information
C) Constructing online surveys
D) Engineering software for social media

22. What type of identity theft uses someone else’s information to obtain medical care?
A) Financial theft

B) Medical identity theft
C) Tax fraud
D) Credential fraud

23. Which is a common method for criminals to steal your mail?
A) Dumpster diving
B) Mail theft
C) Shoulder surfing
D) Hacking social media

24. What is “data breach”?
A) A system crash
B) Unauthorized access to a database containing personal information
C) A leak in a water pipe
D) Losing your laptop

25. Which of these is NOT a secure practice for online accounts?
A) Using multi-factor authentication
B) Reusing passwords across sites
C) Choosing strong, unique passwords
D) Regularly monitoring account activity

26. Which document is most often used to verify identity in financial transactions?
A) Passport or driver’s license
B) Library card
C) Birth certificate
D) School ID

27. What is a “fraud alert”?
A) A warning to friends about spam emails
B) A notice to credit bureaus to monitor accounts for suspicious activity
C) An alert on social media
D) A general news warning

28. Which type of identity theft involves creating a new identity using a combination of real and fake information?
A) Financial theft
B) Synthetic identity theft
C) Tax fraud
D) Account takeover

29. Why is it dangerous to use public Wi-Fi for online banking?
A) Wi-Fi is slow
B) Hackers can intercept sensitive information transmitted over unsecured networks

C) It costs money
D) It drains battery

30. What is “dumpster diving” in the context of identity theft?
A) Disposing of trash safely
B) Searching trash for documents containing personal information
C) Collecting recyclables
D) Hunting for lost pets

31. How can you protect sensitive documents at home?
A) Store them in a safe or locked drawer
B) Leave them on the desk
C) Throw them in the trash
D) Give them to a neighbor

32. What is “credential stuffing”?
A) Memorizing multiple passwords
B) Using stolen usernames and passwords to access accounts
C) Collecting email addresses
D) Organizing credentials for personal use

33. Which personal information should you NEVER share on social media?
A) Birthdate and address
B) Favorite movie
C) Pet’s name
D) Hobby

34. What is the primary purpose of identity theft monitoring services?
A) To sell your personal data
B) To detect unauthorized use of your personal information
C) To clean your credit cards
D) To offer discounts

35. What is “mail fraud” in identity theft?
A) Sending spam emails
B) Using stolen mail to commit identity theft or financial fraud
C) Misaddressing mail
D) Ordering things online

36. Which of these is a secure method for disposing of old electronics?
A) Throwing them in the trash
B) Donating without wiping data
C) Factory resetting and properly recycling
D) Leaving them outside

37. Why is it risky to overshare personal information online?

A) It helps marketers
B) It can be used by identity thieves to impersonate you
C) It improves social media engagement
D) It boosts creativity

38. What should you do if your Social Security number is compromised?
A) Do nothing
B) Report it to the Social Security Administration and monitor accounts
C) Change your name
D) Only inform friends

39. What is the role of banks in preventing identity theft?
A) They are not involved
B) They implement security measures like alerts, fraud detection, and identity verification
C) They report customers to the government
D) They sell information

40. Which of these is a red flag for phishing emails?
A) Misspellings and generic greetings
B) Correct grammar and personalized addresses
C) Trusted company domain
D) Familiar contacts

41. What is “medical identity theft”?
A) Using someone’s personal info to get medical services or prescriptions
B) Pretending to be a doctor
C) Stealing medical equipment
D) Copying medical research

42. What is “account cloning” in identity theft?
A) Duplicating your own bank account
B) Creating a copy of someone else’s account to commit fraud
C) Opening a joint account
D) Copying social media profiles for fun

43. Which of the following is NOT a common identity theft target?
A) Social Security numbers
B) Credit card numbers
C) Library card numbers
D) Medical insurance information

44. What is “tax refund fraud”?
A) Filing false tax returns using someone else’s information
B) Filing taxes late
C) Forgetting to claim deductions

D) Filing for a smaller refund than eligible

45. Which type of identity theft involves using your name to open credit cards or loans?
A) Medical identity theft
B) Financial identity theft
C) Credential theft
D) Employment identity theft

46. What is the safest way to dispose of old credit or debit cards?
A) Throwing them in the trash whole
B) Cutting or shredding them
C) Giving them to friends
D) Melting them

47. Which of the following is a sign that your email account might be compromised?
A) Unexpected password change notifications
B) Receiving emails from friends
C) Low storage warnings
D) Frequent login from your own device

48. Why is multi-factor authentication (MFA) effective?
A) It uses multiple devices to log in
B) It requires a second verification step beyond a password
C) It increases storage space
D) It improves Wi-Fi speed

49. Which of the following is an example of “pretexting”?
A) Creating a fake scenario to trick someone into giving personal info
B) Fishing in a lake
C) Reading someone’s emails without permission
D) Copying software illegally

50. What is “online impersonation”?
A) Pretending to be someone else online for fraudulent purposes
B) Creating a social media account
C) Posting opinions online
D) Using emojis in a message

51. Which of these is a proactive step to prevent identity theft?
A) Monitoring your credit report regularly
B) Posting your address online
C) Using the same password everywhere
D) Ignoring emails from banks

52. What is the role of the Federal Trade Commission (FTC) regarding identity theft?
A) Investigating and providing resources for victims
B) Prosecuting criminals directly
C) Offering free bank accounts
D) Tracking online ads

53. What is “SIM swapping”?
A) Exchanging SIM cards with a friend
B) Hijacking your phone number to access accounts
C) Upgrading to a new SIM card
D) Changing your mobile plan

54. Which type of identity theft involves using a person’s info to gain employment?
A) Medical identity theft
B) Employment identity theft
C) Tax identity theft
D) Social media theft

55. Why is it dangerous to click links in unsolicited emails?
A) They might be fun
B) They can lead to phishing or malware attacks
C) They improve internet speed
D) They delete emails automatically

56. What is “identity cloning”?
A) Creating fake identities for research
B) Copying all personal info of a victim to use fraudulently
C) Making photocopies of ID
D) Sharing ID with family

57. Which of the following is a sign of identity theft related to your credit report?
A) Unknown accounts or inquiries
B) Your own accounts listed correctly
C) No updates for months
D) A higher credit limit

58. What is “pharming” in cybersecurity?
A) Planting crops online
B) Redirecting users to fraudulent websites to steal information
C) Email phishing
D) Logging into a bank account

59. Which of these is an effective password management strategy?

A) Using a password manager to create unique, complex passwords
B) Writing passwords on a sticky note
C) Using “password123” everywhere
D) Sharing passwords with friends

60. How long should you keep documentation when resolving identity theft?
A) Until the case is resolved and some extra time for verification
B) Only one day
C) Only electronically
D) Never

61. What is “dark web” identity theft?
A) Theft of identities for sale or trade on hidden internet sites
B) Stealing printed documents
C) Accessing social media
D) Losing passwords at home

62. Which of the following is a method to protect your identity online?
A) Regularly updating software and security patches
B) Using the same password for all accounts
C) Clicking on pop-up ads
D) Using public computers for banking

63. What is “identity fraud alert”?
A) A notification system to alert the credit bureau and lenders of suspected fraud
B) A social media notification
C) A marketing alert
D) An email spam warning

64. Which of these is an example of “child identity theft”?
A) Using a child’s Social Security number to open credit accounts
B) A child losing their library card
C) A child posting online
D) A child sharing a password

65. How can malware contribute to identity theft?
A) By stealing passwords, banking info, or other personal data from your device
B) By slowing down your computer only
C) By deleting files
D) By creating art

66. Which type of identity theft involves stealing personal information to open fake social media accounts?
A) Social media identity theft

B) Medical identity theft
C) Tax identity theft
D) Employment identity theft

67. What is “credit card skimming”?
A) Stealing card information from ATMs or point-of-sale machines using a device
B) Ripping off the magnetic strip of your own card
C) Losing a card in the mail
D) Checking balances quickly

68. Which of the following is a strong password?
A) MyBirthday123
B) 1q2w3e4r
C) H#7vP!2z&9x
D) password

69. What is a common method identity thieves use to gain access to personal info online?
A) Phishing emails
B) Using antivirus software
C) Logging in from home
D) Watching TV

70. Which of the following actions is important after discovering identity theft?
A) Notify banks, creditors, and credit bureaus
B) Wait a few months before acting
C) Delete your social media
D) Ignore emails

71. What is “online scam baiting”?
A) Pretending to fall for scams to expose or catch scammers
B) Ignoring scams
C) Paying scammers
D) Reporting scams only

72. What does a “security breach notification” usually indicate?
A) Your personal data may have been exposed
B) A new software update
C) A marketing promotion
D) Your email is full

73. What is “account monitoring” in the context of identity theft prevention?
A) Checking accounts for suspicious activity regularly
B) Sharing your password
C) Deleting old emails

D) Logging into your account once a year

74. Which of these is an example of a physical identity theft method?
A) Stealing a wallet or mailbox
B) Using a fake website
C) Phishing emails
D) Malware

75. Which is NOT a recommended way to verify an online website's security?
A) Look for "https://" in the URL
B) Check for a padlock icon
C) Verify the domain spelling
D) Enter sensitive info without checking the URL

76. How does "identity theft insurance" help victims?
A) It reimburses costs related to restoring your identity and financial loss
B) It prevents all thefts automatically
C) It tracks online activity
D) It cancels debt automatically

77. Which type of fraud uses stolen identities to obtain employment illegally?
A) Employment identity theft
B) Tax fraud
C) Social media theft
D) Credit card fraud

78. What is a key step in recovering from identity theft?
A) Filing an identity theft report with the FTC or local police
B) Ignoring the issue
C) Deleting social media accounts
D) Changing hobbies

79. Why is it risky to answer unknown calls asking for personal information?
A) It wastes time
B) It could be social engineering to steal information
C) They may be telemarketers
D) It causes phone overheating

80. What is "password spraying"?
A) Trying common passwords on multiple accounts to gain unauthorized access
B) Sharing passwords with friends
C) Changing passwords frequently
D) Using a password manager

81. Which of the following is considered a strong safeguard for online accounts?
A) Multi-factor authentication (MFA)

B) Using “123456” for all accounts
C) Sharing passwords with family
D) Logging in from public Wi-Fi

82. Which of the following is a warning sign that someone may have opened accounts in your name?
A) Receiving bills for accounts you didn’t open
B) Getting a regular paycheck
C) Notifications from friends
D) Seeing social media ads

83. Which government resource helps identity theft victims in the U.S.?
A) Federal Trade Commission (FTC)
B) Department of Transportation
C) NASA
D) Social Security Administration only

84. What is “data scraping” in identity theft?
A) Collecting personal info from websites or social media for fraudulent use
B) Cleaning computer screens
C) Deleting old emails
D) Backing up data

85. Which of the following is NOT recommended when creating a secure password?
A) Including numbers and symbols
B) Using at least 12 characters
C) Using easily guessable information like birthdates
D) Using both upper and lowercase letters

86. Which action is effective to prevent mailbox theft?
A) Using a locked mailbox or USPS hold services
B) Leaving mail on the porch
C) Sharing your mailbox key
D) Ignoring mail notifications

87. What is “identity theft recovery kit”?
A) A set of instructions and tools to report and recover from identity theft
B) A medical kit
C) A software program
D) A set of passwords

88. Which type of identity theft uses someone’s information to commit online fraud in games or virtual economies?
A) Digital/virtual identity theft
B) Medical identity theft

C) Employment identity theft
D) Tax fraud

89. Why should you regularly check your bank and credit card statements?
A) To catch unauthorized transactions early
B) To increase spending
C) To compare advertisements
D) To decorate your desk

90. What is “business email compromise” (BEC)?
A) Scammers impersonating business contacts to steal money or data
B) Sending marketing emails
C) Employee emails being too long
D) Hackers installing viruses

91. Which is a step in recovering from identity theft involving accounts?
A) Contacting banks and creditors to freeze or close fraudulent accounts
B) Ignoring notifications
C) Posting on social media
D) Giving up online accounts

92. How can you protect children from identity theft?
A) Monitor personal info usage, avoid sharing SSNs unnecessarily, and review credit reports for minors
B) Give them full access to online accounts
C) Share their information freely
D) Ignore any unusual activity

93. What is a common consequence of identity theft?
A) Financial loss and damaged credit
B) Free vacations
C) Lower utility bills
D) Extra social media followers

94. Which of the following helps protect against SIM swapping attacks?
A) Adding a PIN to your mobile account
B) Sharing phone number publicly
C) Ignoring account alerts
D) Using default passwords

95. Which action is recommended when a company notifies you of a data breach?
A) Change passwords and monitor accounts for suspicious activity
B) Ignore the notification
C) Delete your accounts immediately
D) Share the news publicly

96. What is the main risk of oversharing personal info on social media?
A) It can be used to answer security questions or guess passwords
B) It increases followers
C) It improves internet speed
D) It reduces spam

97. Which of these is a red flag of identity theft in your credit report?
A) Accounts you did not open
B) Your own account balances
C) Old loans being paid off on time
D) Correct credit inquiries

98. What is a “fraud victim statement”?
A) A document explaining the theft for banks and credit bureaus
B) A social media post
C) A bill
D) A press release

99. Which step helps prevent identity theft from online shopping?
A) Use secure websites (HTTPS) and trusted payment methods
B) Click random ads
C) Save credit card info on all sites
D) Share your card with friends

100. What is the first step to take if you become a victim of identity theft?
A) Document the situation, contact banks and authorities, and file an identity theft report
B) Panic and do nothing
C) Ignore all communications
D) Close your email account only