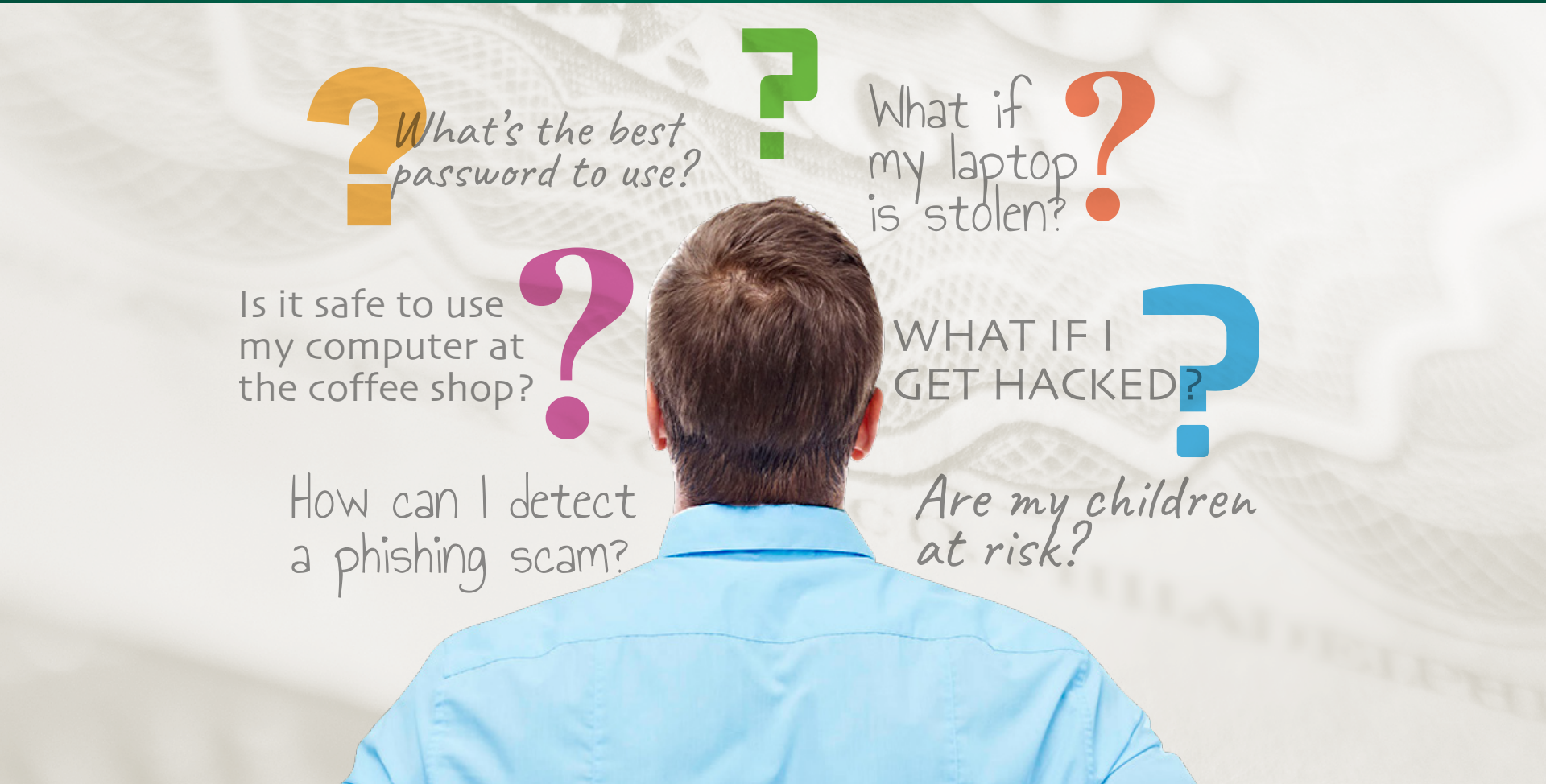
TEST *Your Cybersecurity* I.Q.



QUESTION:

1. A good password to use for logging into your online banking website is:

a) 123456789
b) Password
c) 1Banana+1Pineapple
d) None of the above

Source: FDIC Consumer News, Winter 2016

ANSWER:

c) 1Banana+1Pineapple

Experts recommend creating "strong" user IDs and passwords for your computers, mobile devices and online accounts by using combinations of upper- and lower-case letters, numbers and symbols that are hard to guess. In our example, "1Banana+1Pineapple" would be a good password because it could be easy for you to remember and difficult for others to guess. You should also change your passwords on a regular basis.

Source: FDIC Consumer News, Winter 2016

QUESTION:

2. It's always safe to use your laptop computer or other mobile device to access your online banking site from a coffee shop, airport or other public place that promotes the use of its Wi-Fi network. True or False?

a) True

b) False

Source: FDIC Consumer News, Winter 2016

ANSWER:

b) False.

Not all public Wi-Fi networks are up to date with anti-virus and other security precautions that could prevent cyberthieves from stealing information that can be used to commit crimes. For sensitive matters such as online banking, consider only accessing the Internet using your own computer with a secure, trusted connection, and only connecting laptops and mobile devices to trusted networks.

Source: FDIC Consumer News, Winter 2016

QUESTION:

3. In case your tablet, computer or smartphone is lost or stolen, which of the following precautions would NOT be a good way to restrict access to your device and the data on it?

a) Use a password to restrict access.
b) Add an “auto lock” feature that secures the device when it is left unused for a certain number of minutes.
c) Add a GPS tracking system for your mobile device.
d) Download an app that enables you to remotely wipe data from the device.

Source: FDIC Consumer News, Winter 2016

ANSWER:

c) Add a GPS tracking system for your mobile device.

Passwords and auto-lock and remote-wipe features are good ways to prevent a criminal from accessing your device and data. It's also a good idea to back up your data in case you don't get your device back. Although you can add a GPS tracker to a tablet or smartphone for help locating and recovering the device, it won't prevent a thief from accessing account numbers and other important data.

Source: FDIC Consumer News, Winter 2016

QUESTION:

4. Parents and guardians should ensure that the devices their children use have the latest security updates from the software manufacturer. Which of the following equipment should have the latest security updates?

a) Computers
b) Tablets
c) Smartphones
d) Video game devices
e) All of the above

Source: FDIC Consumer News, Winter 2016

ANSWER:

e) All of the above.

Any device that can connect to the Internet, including video games, needs security updates.

Source: FDIC Consumer News, Winter 2016

QUESTION:

5. You receive an email offering you a free entry in a million-dollar sweepstake if you click on a link that leads to an entry form. It's safe for you to:

a) Click on the link but not download the attachment (the supposed entry form).
b) Delete the email without clicking on the link.
c) Do either of the above.

Source: FDIC Consumer News, Winter 2016

ANSWER:

b) Delete the email without clicking on the link.

Delete the email without clicking on the link or opening the attachment, which could contain "malware" (malicious software) that a criminal can use to monitor your keystrokes, learn your online banking information and move money out of your account. And, just clicking on the link may be enough to download malware onto your computer.

Source: FDIC Consumer News, Winter 2016

QUESTION:

6. Never include your birthday on your social media pages. True or False?

a) True
b) False

Source: FDIC Consumer News, Winter 2016

ANSWER:

b) False.

While cybercriminals can use facts such as your birthday or your place of birth to help them figure out passwords to online accounts, experts say it is OK to provide that kind of information on your social media pages but only if you have adjusted your security settings to prevent strangers (especially criminals) from seeing these details.

Source: FDIC Consumer News, Winter 2016

QUESTION:

7. FDIC deposit insurance will not protect my deposits in the event that a thief online (or otherwise) takes money from my account. True or False?

a) True

b) False

Source: FDIC Consumer News, Winter 2016

ANSWER:

a) True.

FDIC deposit insurance only protects deposits if an FDIC-insured institution fails; it does not cover thefts from accounts. However, other federal consumer laws and financial industry practices may protect theft victims from losses, especially if they have been paying attention to their account activity.

Source: FDIC Consumer News, Winter 2016

QUESTION:

8. If a thief uses one of your small business' debit cards to make fraudulent purchases online, your protections against loss from cyberattacks are the same as those for your personal debit card. True or False?

a) True

b) False

Source: FDIC Consumer News, Winter 2016

ANSWER:

b) False.

Debit cards issued for business use are covered by different loss protections than those for debit cards for consumers. Business debit cards are covered by the Uniform Commercial Code (UCC), which sets many rules for businesses.

Source: FDIC Consumer News, Winter 2016

Protect Yourself and Your Family
from Online Threats.

For More Help or Information
on Cybersecurity
Go to www.fdic.gov/consumersecurity
or Call the FDIC Toll-Free at 1-877-275-3342

Source: FDIC Consumer News, Winter 2016