Fraud Prevention Quiz

1.
Social networking on websites can be a fun and convenient way to meet people and stay connected. What information do you include on your social networking profile?
(Select all that apply)

- [ ] My date of birth, including the year
- [ ] My phone number
- [ ] My physical address
- [ ] None of this information appears publicly on my profile
- [ ] None, I do not have a social networking profile

2.
Are you reviewing your credit report annually or subscribing to a reporting service that notifies you of changes to your credit report?

- ○ Yes
- ○ No

3.
Which of the following kinds of documents do you shred before throwing away?
(Select all that apply)

- [ ] Unwanted credit offers
- [ ] Transaction and ATM receipts
- [ ] Cancelled checks
- [ ] Financial statements
- [ ] Expired bank cards
- [ ] None, I do not shred these items

4.

Answer True or False to the following statements:

I receive my financial information (bank statements, credit card statements, checks, or other notices) online or in a secure mailbox.

- ○ True
- ○ False

I review financial statements or account activity online regularly and report any discrepancies or suspicious transactions immediately.

- True
- False

5.
In the past month, have you updated the anti-virus software on your computer(s)?

- Yes
- No

6.
Libraries, copy centers, and other locations have computers available for public use. Do you use these computers to access personal or financial account information?

- Yes
- No

7.

Answer True or False to the following statements regarding your online banking password:

I change my password regularly (every 30 to 60 days).

- True
- False

I use my date of birth, Social Security number, or other personal information for my password.

- True
- False

I choose passwords that contain a combination of letters, numbers, and special characters.

- True
- False

8.

Imagine you receive an email with the following message:

EMAIL CHANGE NOTIFICATION

Dear Customer!

Thank you for banking online at wellsfargo.com. Our records indicate that you recently added or made a change to your email address(es). This notification is to confirm that you initiated this change.

If you feel you have received this email in error and did not add or change your email address(es), please click here.

Sincerely,
Online Banking Team

What are you most likely to do?

- Click on the link and sign into an online banking session
- Respond to the email sender asking for more information
- Delete the email
- Forward the email to reportphish@wellsfargo.com and then delete it
- Send it to a friend to see what she thinks

9.

Mobile banking applications are programs you can download to your mobile device. If you have suspicions about the authenticity of a mobile banking app, what should you do?
(Select all that apply)

- [ ] Download it anyway because tools on the Web are always safe
- [ ] Contact the financial institution for instructions on how to access its mobile app
- [ ] Conduct your banking through the official mobile website instead of using the app
- [ ] Don't download the app
- [ ] Verify that the name of the app publisher is correct

10.

If you receive a phone call from someone who claims to be an employee of your bank and the caller asks for your Personal Identification Number (PIN) or other confidential information, what would you do?

- Provide the information requested so your bank can confirm your identity
- Do not provide any information, ask the caller for the purpose of the call, and contact the bank directly regarding this inquiry