Banking locally EVER AFTER IS KEEPING YOUR INFORMATION SAFE

SOCIAL ENGINEERING

Social engineering is a type of fraud that exploits your natural inclination to trust the people you know. These scams can occur online or in person. On social networks and websites, fraudsters posing as your friends and colleagues can fool you into revealing your personal information.

Because social engineering attacks look legitimate, they can be difficult to detect. Learn how to identify this deception and avoid becoming a victim.

Search for Fake Accounts in Your Name

Periodically search to see if someone has created a fake account using your name or personal information on social media. By checking common search engines for your name and keywords or phrases (such as your address), you may turn up evidence that someone is using your information in a dishonest way.

Learn to Use Privacy Settings

Use privacy settings to make your social networks accessible only to people you know. Never make your entire profile visible to everyone. By actively managing your privacy settings, you can help to ensure that your personal information doesn't fall into the wrong hands.

Keep Some Things to Yourself

Avoid posting detailed personal information about yourself, such as your:

- Full birthday
- Street address
- Financial account numbers
- Government document numbers, such as Social Security, driver's license and passport
- Information commonly used for security questions, such as your mother's maiden name

A dedicated cybercriminal can learn enough about you through just one or two pieces of sensitive information to steal your identity.

Be Suspicious of New Connections

Think before you accept a new connection from someone whose name you don't recognize; it could be a fake request. Consider accepting connection requests only from people you've met or from those who were referred by trusted connections.

Pick Up The Phone

Ignore emails or profile updates that seek private details such as IDs or account numbers. If you think the request might be legitimate, then call the organization—using a number you know to be valid—and offer to answer over the phone.

Beware of Software Downloads

Download software only from trusted sources—be wary of file-sharing sites or "free" offers. Treat software downloads on social media with the same suspicion as offers received through unsolicited email.

Additionally, some organizations may monitor your Internet behavior through (often free) software downloaded to your computer or public computers. Although you may have i ntentionally downloaded this software, you may not be aware of the tracking software that comes with it.

Be especially skeptical of downloading software containing offers such as free "virus protection" or "PC performance accelerator." In exchange, you may be compromising the privacy and security of your online financial transactions.

Carefully read the end user license agreement (EULA) covering software to make an informed decision that takes into account any privacy and security issues. Consider asking your friends about software or an app first to learn if they had any problems.

Use Security Questions Wisely

When choosing security questions, you'll want to make sure they can't be easily guessed. For instance, only you and your close friends would know the answer to "What was the name of your first pet?" However, an enterprising fraudster might be able to guess "What was your high school mascot?" or "Who is your favorite superhero?"

Look Before You Click

Criminals can hide the destination of a link, so even though the text reads "Visit ABC Corp," the link might actually go elsewhere. Mouse over the link and check the information bar at the bottom of your browser to see where it really goes.

Beware of Phone and Text Scams

Criminals also use phone calls and text messages to impersonate someone else and trick you into revealing information. Examples include tax audit, tax refund and tech support scams.Don't rely on the caller ID display because it can be changed to mask a call's true origin. Criminals can also easily set up a toll-free number with an automated system to gather payment card or Social Security numbers.

Ignore phone calls or text messages that urge you to provide your account number and other personal information to prevent dire consequences like account closing, tax penalties or arrest.

Need help?

If you believe that you may have supplied your account information in response to a social engineering scam, contact your financial institution immediately.