Security Tips

Manage your passwords

Choose complex passwords that aren't obvious: Not your birthday, or your dog's name. Don't use the same password for every account. Update them frequently.

Many consumers use password managers, programs that generate strong passwords and store them securely.

Obviously, if you get a warning that your password was compromised in a breach, find a new one.

Set alerts

Your bank probably has an alerts page, where you can choose to receive a text message or email if someone changes your password or contact information.

An account alert can tell you about a withdrawal, declined transaction, or any activity above a certain dollar threshold.

Beyond passwords

Many financial institutions use two-factor authentication as a way to double-check your identity.

The obvious example is those numeric codes you get on your cellphone when you try to log in, in case someone has stolen your password.

More institutions are using biometrics, such as facial recognition and fingerprint software, to prove beyond any doubt that it's you.

Such measures "may take a little longer," J.D. Power reports, "but the protection is worth the hassle."

Update your app

Make sure you have the most recent version of your banking app on your smartphone. The app will usually tell you when it's time to update.

Go paperless

Paperless correspondence saves time and effort. It's also safer, security experts say, because there's no paper trail for a criminal to follow.

Don't share your smartphone

Be careful with your phone "Because the phone is really the key to your kingdom."

Don't share your phone. Don't leave it lying around, unlocked, where people can access it.

If you're buying something on a payment app, complete the transaction yourself. Don't hand your phone to the person making the sale.

More: Scam losses worldwide this year are $1 trillion. How to protect yourself.

Beware of the unexpected

Be careful about answering an email, call, or text that claims to be from your bank. The American Bankers Association lists five red flags:

- A message with a link you weren't expecting.
- Anything using urgent or fretful language.
- Any attachment.

Security Tips

- Any request for personal information, like a PIN or password.
- Anything that pressures you to send money on an app.

“If you didn’t expect it,” Ehresman said, “don’t click on it.”

This article originally appeared on USA TODAY: Bank fraud is rampant. Your data could be anywhere. Here's how to protect yourself.