# 8 TIPS FOR BANKING ONLINE SAFELY

## 1 Monitor your accounts regularly.

Make sure that all transactions posted are ones you have authorized. Report any suspected fraudulent or suspicious activity to your bank immediately.

## 2 Look out for strange emails!

Don't respond to emails that claim to be from your bank (or any other company) requesting your account details or passwords. **Banks will not reach out to you over email to ask for your account details.**

## 3 Avoid clicking links in emails.

It is usually much safer to log in to your bank website manually to ensure you are entering a secure site.

## 4 Change your bank passwords regularly.

Avoid using the same password across multiple sites and make sure you are choosing a strong password that is a mix of upper and lower case letters, numbers and special characters. Avoid using any words or phrases that contain your name, initials or your birthdate.

## 5 Enable two-factor authentication.

Many financial institutions have added a layer of security for account holders. Two-factor authentication requires you to enter an extra verification credential before you can access your account.

## 6 Disable automatic login.

Do not allow your web browser to store private username and password information for your online banking websites.

## 7 When available, only use your bank's official mobile apps.

And make sure you download apps from reputable sources such as the Apple Store or Google Play Store.

## 8 Not sure if something is legitimate?

Do you have questions about your bank's technology? Call them—they will be happy to help!

**Brought to you in collaboration by:**

THE STATE OF TEXAS DEPARTMENT OF BANKING

Texas Bankers Association

# 8 TIPS TO BE MORE CYBERSECURE

## 1 Email Fraud

If it seems too good to be true, it is probably fraud. Don't believe that lottery awards staff or princes from a foreign country will contact you by email!

## 2 Fraudulent Payments

Be on guard against fraudulent checks, cashier's checks, money orders or electronic fund transfers sent with a request for you to wire back part of the money.

## 3 Unsolicited Offers

Be wary of unsolicited offers that require you to "ACT FAST."

## 4 Stay Up-To-Date

Make sure your device is up-to-date with the latest security updates for your operating system — Windows, Apple IOS, mobile phone IOS (Apple, Android, etc).

## 5 Warnings and Errors

Do not trust websites with certificate warnings or errors.

## 6 Beware of Email Attachments

It's never a good idea to click on an email attachment or free software from unknown sources. You could end up exposing your system to online fraud and theft.

## 7 Sharing Online

Watch how much you share online. The more you post about yourself on social networking sites, the easier it may be for someone to use that information to access your accounts, steal your identity and more. Protect your personal information by maximizing your privacy settings.

## 8 Financial Scams

Be aware of disaster-related financial scams. Con artists take advantage of people after catastrophic events by claiming to be from legitimate charitable organizations when, in fact, they are attempting to steal money or valuable personal information.

**Additional resources about being safe online:**

Texas Department of Banking – www.dob.texas.gov
Texas Bankers Association – www.texasbankers.com/BankingSafely
Better Business Bureau – www.bbb.org/council/for-businesses/cybersecurity/