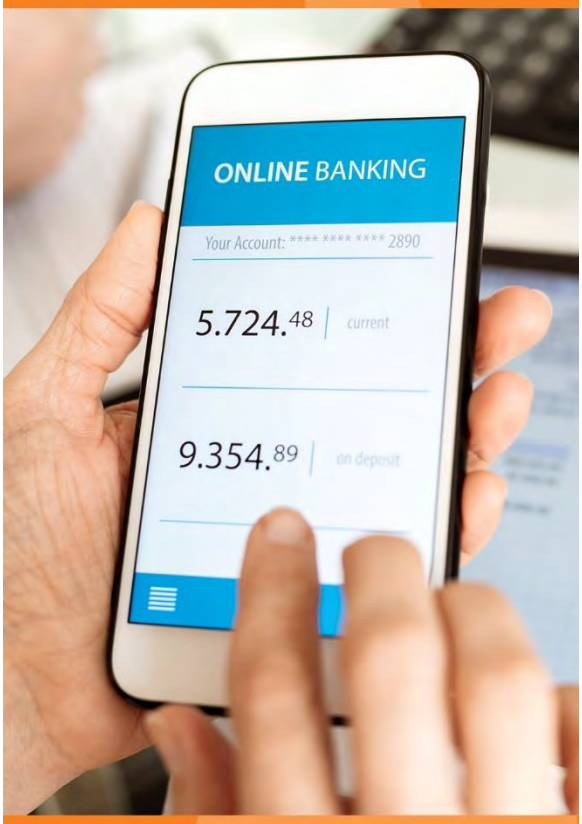
Cyber Safety Guide



Texas Bay
CREDIT UNION

Texas Bay's Cyber Safety Guide

Table of Contents

Texas Bay's Cyber Safety Guide

As the use of digital banking increases, so does the cost of cybercrime. Here are some statistics.

+31% Increase
In cyber attacks from 2020 to 2021

5.9 Million
Fraud reports in 2021

$10.5 Trillion/yr
Expected annual cybercrime costs by 2025

$56 Billion
2020 losses from ID theft victims

1 Billion
Emails were exposed in a single year

1 in 2 American Users
Accounts breached in 2021

MOST COMMON SCAMS

Imposter Scam

What it is: Scammers will contact victims pretending to be from a bank, a government agency like the IRS or Medicare, or a charitable organization to try to get money or personal information that can be used to sell on the dark web. They may ask for payment for things like owing back taxes or having an unpaid debt that needs to be settled immediately.

How to Protect Yourself: Watch out for anyone reaching out to ask for personal information to verify your account, or asking for payment via gift cards, wire transfers, or person-to-person transfers. Legitimate companies will not call to ask for your personal information or for payment.

Urgency Scam

What it is: Any type of scam that pressures victims into taking advantage of a deal or urges them to send a payment, giving a tight timeframe in which to act. Their tone can be urgent, and they may pressure them to provide personal information or send a form of payment by pretending to be hospitals, bail bondsmen, the IRS, or even family members.

How to Protect Yourself: Reputable companies or organizations won't pressure you to act fast with tight time constraints. If an email is asking you to act urgently, take pause. Avoid clicking on any links until you verify if the email is legitimate through a secondary source.

Phishing Scam

What it is: These scams can look like official emails, text messages, social or voice messages from banks or other reputable companies meant to trick unsuspecting victims into giving out personal or financial information to steal personal information or money.

How to Protect Yourself: Look out for generic greetings, misspellings of words, grammatical errors, or variations of logos or names of known companies. If you notice anything suspicious, don't click on any links.

MOST COMMON SCAMS

Utility Scam

What it is: Scammers pretending to be from the electric or other service company will attempt to pressure consumers into sending a payment to avoid having their service turned off. They'll contact victims via phone call or email and use scare tactics to trick those targeted into providing financial information.

How to Protect Yourself: Utility companies will never ask for last-minute payments, especially over the phone or email. If making a payment over the phone, call the utility or service provider directly.

Support Specialist Scam

What it is: Pretending to be a support specialist from a known technology company, scammers try to steal information by claiming there is something wrong with the victim's account or device. These scammers will try to trick victims into thinking that their computer is damaged to get them to allow remote access to scammers under the false claim that they can fix the issue.

How to Protect Yourself: Support specialists from legitimate companies do not cold call to help you fix an issue with a device or account, nor will they ask for consumers to download an app or request access to their device.

Pay Yourself Scam

What it is: Scammers will send a text or email that looks like a fraud alert from the person's bank asking if they authorized a transaction. They then call representing a bank representative offering to help stop the alleged fraud and ask them to send money via transfer or person-to-person payment. In reality, the payment is being sent to the scammer.

How to Protect Yourself: Texas Bay will never call you to verify information or ask you to send money to yourself or anyone. Never give out any personal or account information over the phone or through email.

MOST COMMON SCAMS

Check Overpayment Scam

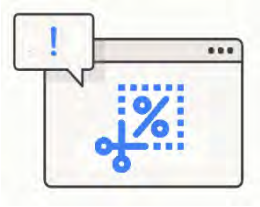
What it is: Fraudulent checks are sent by scammers for a higher amount than expected. They instruct the person to deposit the check and wire a portion of the amount back for reasons like paying for taxes, fees, or supplies. Scammers can target people by pretending to be hiring mystery shoppers or personal assistants, or they may even target people selling items online.

How to Protect Yourself: Don't accept any checks that are for larger amounts than you were expecting. If companies are asking you to send a portion of the check via wire transfers, it's almost certainly a scam.

Automatic Withdrawal Scam

What it is: Scammers will take payment information from free trials that unsuspecting people signed up for from telemarketing calls. They'll then begin to withdraw money from the person's debit or credit account without the victim's knowledge or consent.

How to Protect Yourself: Do not give your checking account number to anyone you don't know, especially over the phone.



Unsolicited Check Fraud

What it is: Scammers will send fraudulent checks that look like rebates or refunds for an overpayment. While these checks are typically for low amounts and can look very real, they're scams that can rope victims into unknowingly enrolling in monthly memberships that are difficult to cancel or high-interest loans.

How to Protect Yourself: Don't cash any check from an unknown sender. Make sure you read everything that came with the check thoroughly, especially any fine print.

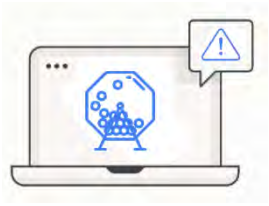
MOST COMMON SCAMS

Romance Scam

What it is: Targeting singles 50+, scammers use fake profiles on dating sites and apps or through popular social media sites, like Facebook and Instagram. They strike up a relationship with you to build trust, sometimes talking or texting several times a day. Then they make up a story and ask for money. They'll tell you to wire money through a company like Western Union, put money on gift cards (like Amazon, Google Play, or iTunes) and give them PIN codes, or send money through a money transfer app, like Zelle® or Venmo.

How to Protect Yourself: Be wary of anyone from a dating or social media site asking for money. Do not send money to someone you've never met. They'll rarely ever meet their target(s) in person.

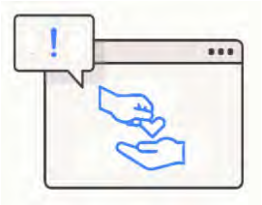
Lottery or Prize Scam



What it is: In a lottery or prize scam, the scammers may call or email to tell you that you've won a prize through a lottery or sweepstakes and then ask you to pay an upfront payment for frees and taxes. In some cases, they may claim to from a federal government agency.

How to Protect Yourself: Avoid providing any personal or financial information, including credit cards or Social Security numbers, to anyone you don't know. Never make an upfront payment for a promised prize, especially if they demand immediate payment.

Charity Scam



What it is: When a thief poses as a real charity or makes up the name of a charity that sounds real in order to get money from you. These scams often increase during the holiday season, as well as around natural disasters and emergencies. Be careful when a charity calls to ask for donations, especially ones that suggest they're following up on a donation pledge you don't remember making.

How to Protect Yourself: Ask for detailed information about the charity, including address and phone number. Look up the charity through their website or a trusted third-party source to confirm that the charity is real. Only give money through the charity's requested donation process.

Texas Bay's Cyber Safety Guide

Today, digital banking is used by just about every age group and demographic. We've taken a look at some of the most common scams that are most prominent by age group.

Youth Bankers

Ages 17 & Under

As of 2020, this group has seen the steepest rise in instances of online fraud with an increase of 116.21% in the number of victims.

Students/Young Adults

Ages 18-29

Between 2019 and 2020, there was a 59% increase in scam victims within this age group, with an average loss of $2,789.

Adults/Parents

Ages 30-59

In 2020, victims of fraud within this age bracket reported monetary losses to romance scames reaching a record $304 million.

Older Adults

Ages 60+

While less likely to report fraud, when they do, this group typically reports a higher amount of monetary loss than younger demographics.

[1]www.seon.io/resources/gen-z-fraud-report-global-outlook | [2]www.bell.bank/advice-center/detail/2020/03/scams-by-life-stage
[3] www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/02/romance-scams-take-record-dollars-2020

Most Common Scams:
Youth Bankers – Ages 17 and Under

Social Media Scams

What is it: Scammers will catfish teens, pretending to be unknown individuals trying to befriend them with the purpose of stealing their personal information or money. They may also target teens by posting fake surveys or contests that can trick teens into giving out personal data.

How to Protect Yourself: Advise teens to set social media accounts to private so information and pictures are not easily accessible to scammers.

Cellphone Freebies

What is it: Scammers will lure teens with "free" wallpapers, ringtones, gift cards, or other items to get them to sign up for their services. However, they may try to get payment information for a processing fee or for shipping and handling, which opts them into expensive, hard-to-cancel subscriptions that teens don't realize they're signing up for.

How to Protect Yourself: Recommend that teens avoid opting into free trials that require payment information upfront.

Online Auctions

What is it: Fraudsters will trick teens into bidding and paying for items that never arrive. Alternatively, scammers will trick teens into sending in their items to sell before they're sold or without an auction taking place. Once they've sent their payment or items, the auction will not take place, and the "representative" of the auction site will disappear.

How to Protect Yourself: Encourage teens to research any auction site thoroughly, including reading previous reviews, making sure the site's contact information is up to date and that they have the appropriate licensing.

Parents: Speak to Your Kids

Youth bankers grew up with computers and smartphones, giving them confidence to navigate the digital landscape with ease. However, they have the least amount of practical experience and are more trusting than other age groups, making them more susceptible to scams.

Parents should have open communications with their youth bankers, educating them on the signs of the most common scams and the danger they pose.

Most Common Scams: Students / Young Adults – Ages 18-29

Online Income Scams

What is it: Fraudsters offer jobs working from home for fast and easy money. After a quick hiring process, they'll send a fake check to the victim's home and ask them to send a portion of the check back. Since financial institutions are required to make funds available, it may be several days before the fake check bounces. By then, the scammer is long gone, and the person is required to pay back the money to the bank/ credit union.

How to Protect Yourself: Walk away from any job offers that require you to send back portions of your check or that ask for any money upfront.

Debt-Related Scams

What is it: Scammers reach out to individuals who may be enticed by the promise that they can get their debts reduced or forgiven –for a steep upfront fee. Victims typically have high credit card debt, a large car loan, or student loans. This relief or reduction of debt never comes, and the victim is robbed of their money.

How to Protect Yourself: Reputable lenders do not require an upfront payment. If a fee is charged, it will always be deducted from the loan before it's disbursed.

Fake Sale Listing Scams

What is it: Services, goods, or apartments are listed on job or community boards for extremely low prices that seem almost too good to be true. Scammers will copy legitimate listings but replace the contact information with their own. Once payment is sent, the perpetrator will disappear without delivering what was promised.

How to Protect Yourself: Unless proven to be a legitimate representative of a company, do not give out any personal information or send payments to anyone you don't know.

What to Remember

Students and young adults are learning to manage their money and the autonomy and responsibilities of growing older, so they may not perceive themselves as targets to scammers.

Personal information should always be guarded and not easily accessible to others.

Most Common Scams: Adults /Parents – Ages 30-59

Mortgage Foreclosure Rescue Scams

What is it: Posing as lenders, loan servicers, etc., scammers will promise to refinance the mortgage, repair credit, or stop a foreclosure. However, they'll request payment for "processing fees" or trick victims into signing documents that transfer the property to these predatory companies.

How to Protect Yourself: Be wary of companies that pressure you into deciding quickly or that say they can guarantee to stop a foreclosure.

Debt Collection Scams

What is it: Scammers pose as law enforcement or debt collectors trying to collect a debt that's not actually owed. They may go as far as threatening jail or even violence to receive payment but refuse to show any written proof of the debt.

How to Protect Yourself: Do not offer any kind of financial information to anyone calling to collect a debt unless you initiate contact first.

Lending Scams

What is it: Like an upfront fee scam, lending scams happen when a victim thinks they're applying for a loan through an online lender or lender app. Scammers then ask for bank information to send a direct deposit. Oftentimes these lenders seek out the individual and don't require a credit check, but they do require an upfront payment for things like "insurance", "paperwork" or "processing fees."

How to Protect Yourself: Be cautious of any lenders who claim to guarantee a loan approval. Reputable lenders will have a set of requirements they abide by.

What to Remember

Adults and parents are Individuals who have years of experience with banking. While they may not have grown up with the internet, they are still familiar and comfortable in the digital landscape. They may not feel like they're vulnerable to scams.

Most Common Scams: Older Adults – Ages 60+

Government Impersonation Scammers

What is it: Scammers use scare tactics to force individuals to wire money, or send a prepaid credit card, gift card, or cashier's check by pretending that they're a trusted individual from a government agency like the Social Security Administration or the IRS. Victims are threatened with jail time, lawsuits, or stopping their social security checks.

How to Protect Yourself: Any government agency will first contact you through the mail, never by phone or email.

Counterfeit Prescription Drug Scam

What is it: Scammers entice the elderly with promises of prescription or "miracle" drugs that can cure certain ailments at a majorly discounted rate but oftentimes the medication never arrives. Besides taking a hit to their financials, these scams may also send counterfeit drugs that could pose a health risk to the victim.

How to Protect Yourself: If purchasing prescriptions online, make sure they're approved by your physician and the National Association of Boards of Pharmacy.

Grandparent Scams

What is it: Scammers trick the victim by pretending to be family, a bail bondsman or an emergency service, notifying that their grandchildren are in dire need of money. They ask unsuspecting victims for funds to be sent through peer-to-peer payments, wire money, transfer funds or use other methods that are hard to trace. These scams can be sophisticated and seem very real. By using information from the internet, the scammer can sound very convincing.

How to Protect Yourself: If you get a call from someone asking for money concerning a family member, hang up and call another family member, service or business using a number from an alternate, verifiable source. Contact local law enforcement to help verify and report fraud attempts.

What to Remember

Adults and parents are Individuals who have years of experience with banking. While they may not have grown up with the internet, they are still familiar and comfortable in the digital landscape. They may not feel like they're vulnerable to scams.

Tips for Your Cyber Safety

Choose Unique Passwords

Avoid using common words, maiden names, or birthdays for passwords. Instead, pick a phrase that can be remembered and add capital letters, numbers, and/or symbols to make it more difficult to decipher. Additionally, passwords should be changed every 90 days and should not be repeated for different logins.

Use Two-Factor Authentication When Available

Employees and customers alike should opt for two-factor authentication to add an extra level of security. Besides adding your credentials when logging in, a code will be sent to your mobile device via text, phone call, or email. This is an additional safety measure so even if you're logging in from a different, unrecognized device, you can ensure that your account is protected. Never share a one-time code with someone with whom you did not initiate contact.

Avoid Public Wi-Fi and Computers

A public network means that anyone can access your accounts, even if they are password-protected. For this reason, avoid accessing your banking app or any other account that can be susceptible to getting breached, like your email. If using a public or shared computer, you should also avoid accessing your bank account online.

Use Licensed Antivirus Software

Keeping your computer updated with strong antivirus software can protect your devices from malware and other cyber threats. Additionally, make sure that all your devices' operating systems and browsers are always up to date since these updates often address bugs and security threats.

Password Protect All Your Devices

Personal or work devices should always be password protected. Like with any password, donot use the same or similar password for all your devices, and do not stay logged in to any of your apps that have sensitive information (like your banking app).

Tips for Your Cyber Safety

Sign Up for Banking Alerts

An easy way to keep track of any transaction in your account so you can spot unusual activity is to get notifications when a purchase above a certain dollar amount is made or whenever money is withdrawn from the account.

Be Vigilant of Phishing Scams

Phishing is when scammers pose as a bank or credit union representative or other trusted company employees to try to get you to divulge personal or financial information to steal your identity or make fraudulent transactions. Typically, banks or other companies already have the information being requested and will not ask their customers for personal information through email, text, or phone.

Avoid Clicking Links in Suspicious Emails

Because sometimes it can be difficult to decipher if an email is legitimate, avoid clicking on links within them. If you need to log in to your bank account, always type the URL of your bank and make sure it starts off with "https:" or a lock icon is present in the URL bar.

Report Incidents to Federal, State, and Local Authorities

If you do fall victim to a scam or if you suspect that you were targeted by a scammer, reporting the incident to Federal, State, and Local authorities can help law enforcement investigate cases of fraud.

Don't Give Out Personal Information

Unless you initiate the call, don't give out any personal or financial information to anyone. Your financial institution or any reputable organization won't ask for this information over the phone, email, or text.

Texas Bay's Cyber Safety Guide

Helpful Resources

Informational

How to Recover After Identity Theft
Fraud Prevention Center
Protect Your Finances
FBI Scams and Safety
Cybersecurity for Small Businesses
Check Your Credit Report

Report Scams

Where to Report Scams
Federal Trade Commission
Texas State Auditor's Office
US Department of Justice
Social Security Administration (suspected scams)
Federal Bureau of Investigation (FBI)

Sources Used for Guide

www.seon.io/resources/gen-z-fraud-report-global-outlook
www.ftc.gov
www.investopedia.com
www.liveabout.com/how-to-avoid-freebie-scams-1357913
www.abc7chicago.com/online-auction-scam-better-business-bureau-scams/11995846
https://oag.dc.gov
www.fdic.gov
www.lendingtree.com/personal/personal-loan-scam
https://consumer.ftc.gov
https://da.lacounty.gov/community/fraud-alerts/prescription-drug-scam
https://consumer.georgia.gov/consumer-education/scams-and-tips
www.usa.gov/common-scams-frauds
www.aura.com/learn/bank-scams
www.wheelingil.gov/210/Automatic-Debit-Scams
www.consumerfinance.gov/ask-cfpb/what-are-some-common-types-of-scames-en-2092