ONLINE SECURITY

Let us help protect you and your business from online fraud, identity theft and more.

Personal Relationships | Local Decisions | Stability

TotalDirectBank®

Member FDIC

2850081759 r07/22

PAYMENT SCAMSONLINE

Don't Be Fooled: How To Avoid SECURITY

Sending Money to a Scammer

Mobile payment apps that provide real-time money transfers, known as P2P, are a convenient way to send and receive money using your smartphone. Mobile payment apps are extremely secure and very popular. Unfortunately, as with so many things digital, there are scammers out there looking for ways to steal your money.

These scammers may try to trick you into sending them money through a mobile payment app. For example, they might pretend to be a loved one who's in trouble and ask you for money to deal with the emergency. Or, they might say you won a prize or a sweepstakes but need to pay some fees to collect it.

Don't be fooled.
Here are ways to avoid being scammed:

1. Transfer money only to people you know and make sure you have the correct phone number or email for that person when making the transfer.
2. Don't respond to texts that ask you to verify transactions unless you confirm the legitimacy of the request.
3. Do not give your account credentials to anyone that contacts you.
4. Protect your account and mobile device with a multi-factor authentication or security code (such as password or token).
5. Before you submit any payment, double check the recipient's information to make sure you're sending money to the right person.
6. Keep your smartphone secure with a strong password, biometric features or two-factor a authentication.
7. If you get an unexpected request for money from someone you do recognize, speak with that person to make sure the request really is from them - not a hacker who gained access to their account.

How to Recover

The internet. Arguably one of the most important contributions to raising the standard of living world-wide in the past 100 years. Responsible for astonishing connectivity, innovation and prosperity.

And with the good comes the bad: cyber criminals engaging in a wide range of illegal activities with one constant - financial loss. Every person, every business, connected to the internet - and who isn't? - is at risk.

Whether you or your business have yet to be directly affected, you can be certain cyber criminals are constantly seeking new targets and vulnerabilities. All with the goal of stealing something of value from you.

How to Stay Safe

Assume the worst. Be prepared. While the threat posed by cyber criminals is very real, there is much you can do to protect you and your business.

TO REPORT IDENTITY THEFT

Equifax Credit Bureau Fraud: **1-800-525-6285**

Experian Information Solutions: **1-888-397-3742**

TransUnion Credit Bureau Fraud: **1-800-680-7289**

Federal Trade Commission: **1-877-FTC-HELP**

Social Security Administration Fraud Hotline: **1-800-269-0271**

Local Police Department

THE ROAD TO RECOVERY

If your identity is stolen, here are some steps you can take to begin the recovery process:

1. Contact all creditors, by phone and in writing, to inform them of the problem.
2. Call each of the three credit bureau fraud units to report identity theft. Ask to have a "Fraud Alert/ Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.
3. Call your local police and your nearest U.S. Postal Inspection Service Office.
4. Alert your banks to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.
5. Contact the state office of the Department of Motor Vehicles to determine if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.
6. Contact the Social Security Administration's Fraud Hotline.
7. Contact the Federal Trade Commission to report the problem (www.ftc.gov)
8. Keep a log of all your contacts and make copies of all documents. You may wish to contact a privacy or consumer advocacy group regarding illegal activity.

BUSINESS PROTECTION

What to do

Enterprise Computers: Desktops | Laptops | Servers

1. Install, maintain and update the strongest possible enterprise-wide antimalware software available. Set antivirus software to run a scan after each update.
2. Install all applications securely. Download software only from official, secure sources.
3. Passwords must be strong and should never be exchanged between users. Use a Password Manager to store passwords, if needed.
4. Whenever users are away from their computers, they should be locked.
5. Unsolicited or "found" removable devices require extra caution. Never connect a removable device to your computer without complete confidence in its origin.

Firewall

1. Make sure your operating system's firewall is enabled.
2. If employees work from home, ensure that their home system(s) are protected by a firewall.

Mobile Device Action Plan

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network.

1. Require users to password protect their devices, encrypt their data, and install security apps to prevent cyber theft while on public networks.
2. Set reporting procedures for lost or stolen equipment.

TotalDirectBank®

Wi-Fi Network Security

1. Make sure the workplace Wi-Fi Network is secure, encrypted, and hidden. To hide your Wi-Fi network, set up the wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID).
2. Password protect access to the router.

Email Security

Phishing attacks, whereby a cyber criminal attempts to gain access to enterprise computer systems through malware embedded in fraudulent emails, is one of the greatest threats and most difficult to defend against. Follow these guidelines to identify and prevent a potential Phishing attack.

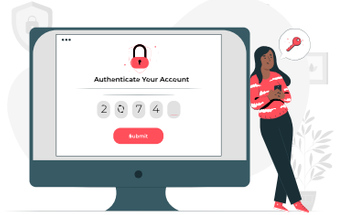
1. Identify the sender of any email received.
2. Carefully review any embedded link before clicking on it. Your default position should be any link is potentially dangerous.
3. Spelling errors, poor grammar, and unusual word choices are reasons for concern.
4. A request for an urgent response is a red flag to slow down.
5. Always err on the side of caution when downloading attachments or clicking on links of any kind.

Hard Copy Records

1. Hard copies of any sensitive or confidential business records should be stored in a safe and secure place.
2. Do not leave sensitive or confidential business records in view on desks or other public spaces.
3. Shred or otherwise destroy hard copies of sensitive or confidential business records no longer needed.
4. Before leaving a meeting room, erase white boards, turn off video screens and remove presentation materials.

Train Employees in Security Principles

1. Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.
2. Having some training in place will help your business manage security expectations for your staff.



PERSONAL PROTECTION

What to do

Computer Equipment, Tablets, Smartphones & Other Internet Connected Devices

1. Install antivirus software.
2. Update all operating systems, browsers and other applications.
3. Download software only from official, legal sources. Be suspicious of any software that is free or dramatically discounted.
4. If you have a camera on your computer or other device, cover it when not in use.

Password Management for Online Services

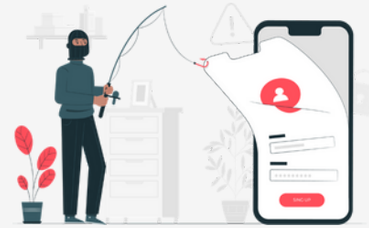
1. Always use strong passwords. A password that is simple for you to remember is often easier for criminals to deduce. Passwords must be strong, a passphrase that is at least 12 characters long. Length trumps complexity and should never be exchanged between users.
2. Use different passwords for different services.
3. Do not save passwords in any browser. Use a Password Manager to store passwords, if needed.
4. Dual factor authentication, if available, is recommended for extra security.

Wi-Fi Service

1. Change the default password provided.
2. Disable the WPS (Wi-Fi Protected Setup) PIN to guard against unauthorized users.
3. Do not expect public Wi-Fi services to be safe and secure. Do not enter private information using public Wi-Fi services.
4. If you use Wi-Fi networks while traveling for business or pleasure, erase the Wi-Fi listings from your device(s) on a regular basis.

Social Networks

1. Be very cautious in interactions and sharing personal information with unknown profiles.
2. Disable geolocation for any photos or images.
3. Always review your privacy options and enable those that give you the most control.



IDENTITY THEFT

Prevention

Identity thieves use a person's specific identifying information to impersonate that person with the intent to commit any number of types of fraud.

Identity theft crimes are serious and may have long lasting effects on the victim's future ability to engage in financial transactions, make important purchases or establish services. The road to recovery may be difficult.

Prevention is Key

Here are some steps to take:

1. Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, bank account number or bank PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessar y.
2. Memorize your social security number and all your passwords and PINs. Do not record them on any cards or on anything in your wallet or purse.
3. Promptly remove mail from your mailbox after delivery, if it does not lock. Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave in unsecured mail receptacles.
4. Shred preapproved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling bin.
5. Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gas pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
6. Report all lost or stolen credit cards immediately.
7. If you have a debit card, check your bank balances regularly to make sure there is no unauthorized use.
8. Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.