partners bank of california

Protecting Your Information - Identity Theft and Online Banking Security Precautions

Identity Theft Precautions

Identity theft is a crime perpetrated by a criminal who uses another's personal information to establish credit, purchase goods and services with existing credit cards, apply for new cards in the victim's name, drain bank accounts or commit other crimes.

Identity theft can affect consumers in many ways; fortunately, there are steps you can take to protect your identity.

How to Protect Your Personal Information

- Never give out personal information, especially your Social Security number, to anyone you can't confirm has a legitimate purpose for asking for it.
- Do not carry your Social Security card, Social Security number, birth certificate or passport with you, unless necessary.
- Do not put your address, telephone number, Social Security number, or driver's license number on personal checks or credit card sales receipts.
- Shred old receipts, credit applications, bank records, and any other personal documents before discarding them.
- Check your credit report at least once a year. Three major credit-reporting agencies (Experian, Equifax, TransUnion) are required to provide you with one free credit report a year. Visit www.annualcreditreport.com to obtain yours.

How to Protect Your Financial Information

- Exercise your rights under the Fair and Accurate Credit Transaction Act and review your credit report regularly to be sure it's accurate and up to date.
- Never give out your password or PIN for your check card, credit card or ATM card.
- Keep important documents in a safe place. Burglars are just as interested in credit cards, bank accounts and investment statements as they are in your other valuables.
- Keep a list of all credit cards and bank accounts including the account numbers, phone numbers and expiration dates in a safe place.
- Provide personal information only on websites that are secure and only when you have initiated the contact.
- Shred financial or confidential information such as credit card preapprovals, credit card receipts, and bank statements.
- Carry only the credit cards you plan to use. If you have credit cards you do not use, store them in a safe place. If you no longer use a particular card, cancel the account and destroy the card.
- Place payments and financial mail in a secured post office box, not in your home mailbox.
- Pick up your mail as soon as possible after it's delivered, and keep track of when your bills are supposed to arrive. If your monthly bank and credit card statements do not arrive in the mail, call your bank or lender immediately.
- Always check bank statements and credit card bills for accuracy.
- Go paperless. Electronic statements and invoices minimize the number of hard copy documents that bear your personal information and could get into the wrong hands.

Steps you can take if you suspect Identity Theft: If you think you are a victim of identity theft, take action immediately. Contact the local police, your bank(s), the three major credit reporting agencies and the Federal Trade Commission at (877) IDTHEFT. Learn more about what to do if you suspect you are a victim of identity theft.

- Immediately change passwords and pins on all possible online profiles, websites, and social media accounts you suspect are compromised. Check your profile on each site to ensure that your cell phone and email address or other contact information has not been altered. If you've used the same password for your online accounts, you risk the exposure of ID Theft across all of those accounts if your email and website viewing history on your PC or devices has also been compromised.
- Notify your financial institutions immediately to report any suspicion of fraud. Review your transaction history on your bank and investment accounts, as well as credit cards to detect any unexpected transactions or sign-on attempts that you did not initiate. Often, banking websites will record the last time your accessed your account online.
- Place a "Fraud Alert" or "Credit Freeze" on your credit reports, and review the reports carefully. A fraud alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing account. Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts on your accounts that you can't explain. The three nationwide consumer reporting companies have toll-

free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:

Experian: 888-397-3742
TransUnion: 888-909-8872
Equifax: 800-685-1111

- Contact the security or fraud departments of each company where an account was opened or charged without your authorization.
- Follow up in writing, with copies of supporting documents. Keep copies of documents and records of your conversations about the theft. Ask for verification that the disputed account has been dealt with and the fraudulent debts discharged.
- Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
- File a police report. File a report with law enforcement officials to help expedite the correction of your credit report and deal with creditors who may want proof of the crime.
- Report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the country in their investigations.

  Online: www.ftc.gov/idtheft
  By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

Identity Theft Resources: Check these resources for more information on identity theft and your credit report:

- Annual Credit Report website www.AnnualCreditReport.com or call 1-877-322-8228
- The Federal Trade Commission (FTC): website www.FTC.gov
- The Federal Deposit Insurance Corporation (FDIC): www.fdic.gov
- Credit Reporting Bureaus: Equifax: (800) 685-1111, Experian: (888) 397-3742, TransUnion: (800) 916-8800

Online Banking and Information Security Precautions

Always access Partners Bank of California's Internet banking by typing in the correct website address **https://www.PBofCA.com** into your browser.

- Never respond to, click any link in, or open an attachment in an email that requests information about you or your accounts, especially unsolicited emails. Instead, type in the source page of the website you intend to visit using a separate tab or window. Question any request to enter personal details, or username and password into a website if you are not sure if the request is legitimate. Criminals can put up a convincing replica of a website with a slight variation in the website address or direct you to a fake site through a link in an email.
- Verify that your banking session is secure: There are two simple indicators that will tell you if your session is secure. The first is the use of https:// in the URL. Some browsers such as Mozilla Firefox change the color of the URL window when you are in a secure session. The other indicator is the presence of a digital certificate represented by a padlock or key in the bottom right hand corner. If you double click on this icon, it should provide you with information about the organization with which you have entered in to a secure session.
- Partners Bank of California may send an email notice or alert; however; we will never ask you to provide any personal or account information via email. We will never ask for your Password.
- You should never send personal or account information by unsecured or unencrypted email.

Password and PIN security: You should always be wary if you receive unsolicited emails or calls asking you to disclose any personal details or card numbers. This information should be kept secret at all times. Be cautious about disclosing personal information to individuals you do not know. Please remember that Partners Bank of California would never contact you directly to ask you to disclose your PIN or all your password information.

- Do not write down your Username or password.
- Do not share your password with anyone.
- Avoid predictable passwords that could be easily guessed by others.
- Use a complex password, and do not use the same password for all of your online profiles. Choose a password you can easily

remember. A complex password may be a phrase, and should include letters (upper and lower case), numbers and symbols.

- Change your password on a regular basis; every 90 days is recommended.
- Avoid storing or saving your password in software or applications.
- Use extra caution when using a public computer.
- Establish Dual Control - For businesses, Partners Bank of California offers "dual control" over your account. Once this safeguard is in place, two individuals from your organization will need to log on and authorize any transaction. With dual control in place, a hacker would need to breach two user accounts in order to commit a fraudulent transaction.

PC Security: It is important to use up-to-date antivirus software and a personal firewall. If your computer uses the Microsoft Windows operating system, it is important to keep it updated via the Windows Update feature, equally if you use another PC operating system or have an Apple Mac you should check regularly for updates. You should be vigilant if you use Internet cafes or a computer that is not your own and over which you have no control.

- **Install antivirus** software AND keep it up to date.
- **Use a firewall.** This can protect against potential hackers and prevent access to questionable connections.
- **Use antispyware.** Often bundled with antivirus software, this can prevent your activities from being monitored and keep your browser from improperly directing you to an unintended site.
- **Disable Scripting.** Unless you create VB Scripts you can disable Script Hosting. This is the weakness exploited by some computer viruses.
- **Disable File sharing.** Any computer with Internet file sharing activated offers its content freely to outsiders. You can easily check and change the setting. From the Start menu select Settings, or Control Panel, then Network and File Sharing. Under the Configuration tab, select TCP IP, click on File and Print Sharing. If either of the two check boxes that appear show ticks, click on them to uncheck them.
- **Apply Patches.** For greater security, apply patches, which are small software add-ons designed to deal with specific security holes and other computer problems. You'll find all the patches you need on your operating system's website.
- **Use a Dedicated Online Banking PC.** Designate a single computer to use as your business's online account machine solely for online banking and not for other activities such as e-mail, web browsing, or file sharing. Infecting a computer is much easier if that computer is regularly connected to the internet or used for email. In particular, the American Bankers Association recommends that "commercial banking customers carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible".

Mobile Device Security: Cybercriminals continue to look for ways to exploit vulnerabilities in apps, operating systems, and software, trying to capitalize on security flaws before manufacturers find and patch them.

- **Regularly update your Operating System (i.e., Windows, Apple, etc.) and apps**. New vulnerabilities are discovered and vendors work to patch their apps and software as soon as available. Also, delete any applications or programs that you no longer utilize.
- **Don't share your mobile device with others** if you have any sensitive financial, banking, or wallet Apps activated on your phone. Allowing others to use your device and register their fingerprint biometric will also incidentally grant them access to your bank accounts if you have enabled fingerprint ID. Most disclosures for online services shift that responsibility back to you to protect your device.
- **Don't use public Wi-Fi** – it may save you from using up your data plan, but unsecured Wi-Fi networks are a significant threat to exposing anything you type or view on your device while signed in to the public Wi-Fi. Never use public Wi-Fi if access requires you to enter personal information.
- **Dodge security and privacy issues via reviewing your app permissions**. Apps sometimes require more than the basic default permissions. Make sure the installed apps only have access to features they need.
- **Set automatic locks on mobile devices.** Ensure that the mobile device locks automatically, and has a strong passcode—a simple pattern or swipe password isn't much of a deterrent. If a device is lost or stolen, a strong password prevents anyone from quickly peeking at personal information.
- **Limit the personal information given to apps and websites.** Signing up for a new service or downloading a new app sometimes requires personal information. Be wary of revealing too much, research how secure the application or site is before logging on.
- **Manage what is shared online.** Make sure to use privacy settings on social media apps and sites. Some sites can broadcast location, email, phone numbers, or more to the public by default.

Be Alert to Common Internet Scams. If it sounds too good to be true - it probably is: Don't be conned by convincing emails offering you the chance to make some easy money. As with most things if it looks too good to be true, it probably is! Be cautious of unsolicited emails from overseas - it is much harder to prove legitimacy of the organizations behind the emails. Train employees: Social engineering is still often used to obtain sensitive information. For example, never trust e-mails requesting personal information such as user names or passwords. If there is no one in the office qualified to provide this type of training, find a trusted IT professional or consultant to educate employees.

- **Phishing** is an internet scam that involves an email which appears to be from a legitimate company, bank, or government agency. The emails typically warn of a potential problem with your account and requests that you follow a link and provide personal or account information to update your information. You should never reply to these emails, open any attachments, or follow any of the links provided. If you believe an email to be legitimate, you should contact the company using your usual contact information.

- **Pharming** is a type of fraud that involves redirection from a legitimate site to a site that appears to be legitimate, but has been created by fraudsters in an attempt to gain your personal or account information.

- **Don't deposit checks and wire money or send money back in any way for others**. Fake electronic deposits and checks drive many types of scams – like those involving phony prize wins, fake jobs, mystery shoppers, online classified ad sales, and others. They individual may have a good story to explain the payment or overpayment of funds– they're stuck out of the country, they need you to cover taxes or fees, you'll need to buy supplies, or something else. But when you've accepted a fraudulent deposit or a bad check, the scammer already has the money, and you're stuck paying the money back to the bank.

Fraud Prevention:

Check your Account Balances each day: Some electronic transactions may not be settled or processed in final until the next business day. If you catch a fraudulent transaction at the end of a business day, you may be able to cancel it before any funds are transferred.

Check your statements: It is important to check your statements regularly; a quick check will help identify any erroneous or criminal transactions that might have been performed on your account without your knowledge.

Segregation of Duties: Businesses can also use dual control when initiating online payments such as ACH and wires, create appropriate payment limits for employees, take advantage of security tokens, assign user transaction limits and call back procedures.

Sign Up for Fraud Prevention products: Set up alerts through online and mobile banking apps may give you early notice that a balance or transaction has posted to your accounts. Business accounts are eligible to sign up for Positive Pay service to help identify check fraud such as paid checks that were never issued, or where the amount was altered. Detecting fraud early is a great way to prevent losses and return items before the 24-hour deadline. Check with your branch or relationship manager if you are interested in Positive Pay or other fraud prevention products.

Confirm payment instructions (or changes to payment instructions) directly with vendors and suppliers: Don't accept a payment change instruction by email, a typical Business email compromise (BEC) scam involves phony e-mails in which the attacker spoofs a message from an executive at a company or a real estate escrow firm and tricks someone into wiring funds to the fraudsters.

Always completely log off from your Internet banking session: It is important to completely log off from your Internet banking session; simply closing the window you performed the transaction in may not close the banking session. If your computer is infected with a Trojan, your session may become hijacked by a criminal and financial transactions performed without your knowledge. It is also advisable to disconnect from the Internet if you are not planning to use it.