partners bank of california

Identity Theft and Online Banking Security Tips Brochure

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 give your Social Security number over a cellular or cordless phone.
- Do not carry your Social Security card, Social Security number, birth certificate or passport, 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 twice 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 credit card bills and bank statements for accuracy.

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.

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

Annual Credit Report Website
The Federal Trade Commission (FTC}: http://ftc.gov
The Federal Deposit Insurance Corporation (FDIC): http://www.fdic.gov

Member FDIC EQUAL HOUSING LENDER

partners bank of california

Identity Theft and Online Banking Security Tips Brochure

Major Credit Reporting Bureaus: Equifax: (800) 685-1111, Experian: (888) 397-3742, TransUnion: (800) 916-8800

Online Banking and Information Security Tips

Accessing PartnersBankCA .com secure website: Always access Partners Bank of California's Internet banking by typing in the correct website address www.partnersbankca.com into your browser. Never click on a link in an email to take you to a website and enter personal details either in the email or website.

- Check 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 Login ID or Password.
- You should never send personal or account information via 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 Login ID or password.
- Avoid predictable passwords that could be easily guessed by others.
- Do not share your password with anyone.
- Include both letters and numbers in your password.
- 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.

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.

Member FDIC EQUAL HOUSING LENDER

partners bank of california

Identity Theft and Online Banking Security Tips Brochure

- Be cautious of links in an email to get to any web page. If there is any question about the legitimacy of the link or the email is from an unknown source, call the company on the telephone at a number obtained independently from the email, to confirm the web page address; or log onto the website directly typing in the web address in your browser, before clicking on the link in question.

PC Security: It is important to use up-to-date antivirus software and a personal firewall. If your computer uses 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 TCPIIP, 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".

Check your Account Balances each day: Automated Clearing House (ACH) transactions are not usually processed 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.

Sign Up for Fraud Prevention products: 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.

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.

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.