Cybersecurity Matters: 
An In-Depth Look at Online Security
Your Security Matters Most

At Pacific Premier Bancorp., Inc. (PPBI) and Pacific Premier Bank, we’re committed to providing each and every one of our clients with exceptional, personalized service. Part of that service includes vigorous, unrelenting, and state-of-the-art cybersecurity protection.

As we continue to expand and evolve in our third decade of operation, we are more devoted than ever before to staying ahead of any and all threats to our clients’ online accounts, presence, and privacy. Cybersecurity threats are real, and they continue to grow and evolve in their complexity, creativity, and reach.

In fact, theft of digital information has become the most commonly reported fraud, surpassing physical theft. And according to Microsoft’s 2016 Trends in Cybersecurity, there are now more than 6,000 software vulnerabilities disclosed each year – with a staggering 41.8 percent of those vulnerability disclosures rated as “highly severe.”

These online threats and thieves aren’t going away anytime soon. Our efforts and executions to recognize, prevent, and eliminate them must be even more aggressive and intelligent.

Inside

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>1</td>
</tr>
<tr>
<td>Passwords</td>
<td>2</td>
</tr>
<tr>
<td>Email</td>
<td>3</td>
</tr>
<tr>
<td>Internet</td>
<td>4</td>
</tr>
<tr>
<td>Wi-Fi Hotspots</td>
<td>5</td>
</tr>
<tr>
<td>Home Networks/Mobile Security</td>
<td>6</td>
</tr>
<tr>
<td>Malware</td>
<td>7</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>8</td>
</tr>
<tr>
<td>Secure Your Credit</td>
<td>9</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>10</td>
</tr>
<tr>
<td>Cybersecurity DOs and DON’Ts</td>
<td>11</td>
</tr>
<tr>
<td>Don’t Waste a Moment</td>
<td>10</td>
</tr>
<tr>
<td>Tech Speak Glossary</td>
<td>12</td>
</tr>
<tr>
<td>Let’s Talk® More</td>
<td>13</td>
</tr>
</tbody>
</table>
Pacific Premier Is Here to Help

ONLINE. ONGUARD. ALL THE TIME.

We Never Stop Safeguarding YOU

Life in modern America doesn’t just happen in one dimension. To live, play, and work in our society today, you need an online identity. And just like in the physical world, it’s important to take steps to ensure your safety and security in cyberspace. It’s equally important to partner with businesses and banks that go out of their way to help ensure your protection online.

Cybercrime has increased exponentially in recent years, and several high-profile cyberattacks, cybersecurity breaches, and information hacks have made the news – and raised red flags and serious concerns among American consumers.

At Pacific Premier Bank, we take your online protection, safety, and security extremely seriously. That’s why our website, www.ppbi.com, supports the strongest encryption\(^2\) hashing algorithm\(^3\) technology available today – SHA256. This online enhancement prevents a cybercriminal from producing fraudulent encryption keys, which can then be used to access your online session via their deceptive tactics.

This is just one of the many ways we demonstrate our relentless and driven dedication to protecting you and your business.

A POWERFUL PARTNERSHIP

Let’s Talk® About Cybersecurity

Of course, there’s strength in numbers. And power in partnerships. We wouldn’t exist without you. And you need us to accomplish all your business banking and growth goals. In the same way, we can join together to help ensure your continued cybersecurity. You can help us help you safeguard your online presence.

---

1 Software Vulnerability: A security flaw, glitch, or weakness found in software or in an operating system (OS) that can lead to security concerns.

2 Encryption: The translation of data into a secret code. Encryption is the most effective way to achieve data security by scrambling the contents into an unreadable form at. To read an encrypted file, you must have access to a secret key or password that enables you to read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

3 Algorithm: A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.
PASSWORDS

Your First Line of Defense

When it comes to guarding against cybercriminals and ensuring cybersecurity at all levels, it’s important to think of your password as your first line of defense. Hackers are becoming increasingly skilled, accomplished, confident, and cunning. They are armed with robust data dictionaries, and dictionaries of words – in both English and other foreign languages. Their ever-evolving strategies and technologies have been estimated to now work effectively enough to break two-thirds of all online passwords. So when fighting back, it’s important to be equally vigilant – and intelligent. Right from the get-go. Right at the first line of defense.

TIPS + TACTICS

- Create strong and unique passwords
- Add complexity to your password with upper and lowercase letters, numbers and symbols
- Remember that longer is better and safer (10-14 characters is ideal)
- Never use dictionary words in your password as those passwords are easy to compromise. A few examples of dictionary words are “password, secret, fishing, baseball, etc.
- Change your password three to four times every year
- Never give your password to anyone – online or off
- Never use your name, social security number, or obvious personal information
- Add an extra layer of security by using spaces in your password
- Keep a record of all your passwords (and store in a safe, secure place)
- Use a phrase instead of a word
- Avoid using the same password for multiple accounts
- Never click on email weblinks that state your password has been compromised and you need to change your password using the weblink
- Always go to the website directly and change your password via the website; and never go through an email weblink, as the email could be fraudulent
EMAIL

Send Hackers Packing
We want to assume our email accounts are safe. After all, email and software providers must provide iron-clad security to any and all accounts, right? Well, not necessarily. No matter how smart or big they are, email providers simply can’t guarantee your cybersecurity when you sign up for their services. Hackers know this to be true. And they strategically attack email providers to gain access to user accounts. Sometimes, they directly attack individual email accounts – using malware, phishing, social engineering, and other assorted scams. Don’t let them get to you. Send them packing with these email security strategies.

TIPS + TACTICS
• Obtain separate email accounts for each of your needs (personal, business, alerts, etc.)
• Use strong and unique passwords that contain at least a symbol, a number and a letter (change often, at least every 90 days)
• Avoid using the same password you use for email accounts on your banking website
• Use data encryption to transmit personal information
• Routinely check your email account settings
• Never send sensitive personal information (i.e. Social Security Number) over email
• Employ spam filters to reduce risk of unwanted and potentially unsafe email
• Beware of unsolicited email; hackers can pretend to be anyone! Always verify with the sender before opening an attachment or clicking a link.
• Where available, enable two-factor authentication in your email service (you’ll then receive an email and/or text when there’s a login from a new computer)
• Only access email accounts from secure networks
• Avoid accessing email accounts from public Wi-Fi hotspots
• Be alert to social engineering email attempts (cybercriminals and scammers pretending to represent established companies)

A Note On Malicious Emails
Exercise extra caution when receiving email messages appearing to originate from banks or financial institutions. Cybercrime has increased significantly in recent years – and malicious email messages claiming to come from trusted entities are designed to deceive you into divulging your nonpublic personal information. Opening file attachments or web links contained in suspicious emails could expose your entire computer system to a costly cyberattack.

To help guard your information from predators, never provide your account information, password or token number over the phone or by email. Pacific Premier Bank will never ask you to enter personal or account information via email or to download an attachment from email, nor will we ever ask you for your password, token or other security credentials via email or by telephone.

---

4Malware: An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

5Phishing: The activity of defrauding an online account holder of financial information by posing as a legitimate company.

6Social engineering: A cyberattack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.
INTERNET

Avoid Information Highway Hijackings
The internet is a complex and globally interconnected network supplying vast amounts of information. Its great strengths are also its major weaknesses. It’s used by just about anyone and everyone you can imagine. There’s no real restriction to jumping on and off. Put simply, every device on the internet can be hacked – many with minimal effort. A common tactic of today’s cybercriminals is to create “clones” of well-known websites, then use them to capture user information and credentials. They then use this stolen information to access your banking and/or other accounts. Don’t crash online. Stay in your lane and drive safe.

TIPS + TACTICS
• Keep your computer software up-to-date
• Keep your cookies⁷ and browser cache⁸ clear
• Maintain at least a “medium-high” level of security on your browser settings
• Look for a “padlock” icon next to a site’s URL in your browser window (indicating a secure/encrypted connection)
• Always log out after doing any online banking (be sure to end/close each session)
• Block ads and pop-ups, and never respond to pop-ups requesting information
• Avoid sites that provide illegal downloads or illegal content (such as file sharing)
• Never download anything from unknown sources/sites
• Only use trusted bookmarks for important sites
• Where available, use two-factor authentication⁹ (you’ll then receive an email and/or text when there’s a login from a new computer)
• Whenever possible, restrict online banking transactions to a computer that is not used for any other website transactions

Microsoft Internet Explorer Alert
Effective January 12, 2016, Microsoft no longer supports, nor provides regular security patches for versions 10 and older of the Internet web browser Internet Explorer. This means that any computers running Internet Explorer version 10 or older will become highly vulnerable to security risks and viruses. If your computer is running Internet Explorer version 10 or older, it is recommended that you upgrade to the latest Internet Explorer version. This will immediately empower you to safeguard the data on your computer against any security threats and viruses that may result from running older web browsers.

---

⁷Cookie: A small file created by a website that is stored in the user’s computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the website to recognize you and keep track of your preferences.

⁸Cache: Portion of a computer’s hard disk space where a browser temporarily stores recently visited webpages to speed up internet surfing.

⁹Two-Factor Authentication: A method of confirming a user’s claimed identity by utilizing a combination of two different components.
**WI-FI HOTSPOTS**

*Why Play with Fire? Find Safer Networks.*

Wi-Fi hotspots have become wildly popular in recent years. And with all the convenience and cost savings they provide, it’s easy to see why. But convenience doesn’t always equate to quality. Or safety. These “hotspots” — and other public Wi-Fi links — have also become popular with cybercriminals and hackers. They love them for their convenience and savings too. They make it easy to collect your logins, emails, and payment information. And in some instances, they help provide free access to all your money. So why take your chances — when you can find safer, secure networks? If you must use Wi-Fi hotspots, here are some helpful tips and tactics.

**TIPS + TACTICS**

- Never use a Wi-Fi hotspot for shopping or banking transactions
- Do not assume that a Wi-Fi link is legitimate or secure
- Do not allow automatic connections to non-preferred networks. Computers, tablets and smartphones can have this setting enabled, please be sure to disable this feature
- Use a Virtual Private Network (VPN)\(^{10}\) service to create an encrypted and secure session
- Before you connect to a Wi-Fi hotspot, be sure to always turn off file sharing
- Before you connect to a Wi-Fi hotspot, make sure to enable a firewall
- Before you connect to a Wi-Fi hotspot, disable ad hoc networking
- Remember that most chat/IM sessions are not secure
- Be aware of your surroundings when online in public spots (look out for “shoulder surfers” watching your screen)

\(^{10}\)Virtual Private Network (VPN): A private network that extends across a public network or internet. It creates an additional layer of security over an insecure network when the network infrastructure alone cannot provide it.
HOME NETWORKS

Play and Stay Safe at Home

It’s only natural for us to feel especially safe and secure while we’re at home. But just as a home intruder might violate your real-world residence, a cybercriminal can “break into” your home network if he or she is skilled and determined enough. Once inside your home network, a cybercriminal can then “rob” you of valuable items like personal data, passwords, IDs, IP addresses,11 account information, and more. To properly and powerfully secure your home network, you should secure the wireless router inside your home. Here are some smart home tips.

TIPS + TACTICS

• Remember that every router comes equipped with a factory-issued username and password. If possible, change the username and/or password.
• Put multi-layered protection in place by changing your router’s name/SSID,12 default password, and wireless network password (network security key)
• Turn on encryption with a strong password (WPA2 is a strong home encryption; WEP is far less secure)
• Set up a primary network for you, and an additional/secondary network for guests
• Stop your router from broadcasting your home network’s name/SSID
• Make sure your router’s firewall is turned on
• Keep your router’s firmware up-to-date
• Use a network monitoring app to scan your network for unwanted users/devices
• Turn off your home’s wireless network when it’s not in use
• Disable “Push-to-Connect” or “WPS” as well as “UPnP” options from your home wireless router. There are many security vulnerabilities around these options that can allow an intruder to connect to your home wireless network without authenticating

MOBILE SECURITY

Secure Your Mobile Devices Too

We live in an increasingly mobile world. Everywhere you go, wherever you look, you’ll find people working, playing, communicating, and connecting on their smartphones, tablets, and other mobile devices. But just how secure from cyberattacks are your mobile devices? Especially if they’re loaded up with social networks and other assorted apps? From Apple to Android, you want to play it safe whenever you can – and wherever you go. Make sure your cybersecurity efforts extend well beyond your desktop or laptop computer with these strategic safety tips for smartphones and mobile devices.

TIPS + TACTICS

• Adjust security settings to restrict others’ wireless- and Bluetooth-enabled access to your data
• If your mobile device has data encryption features, activate and use them
• Install a proven Antivirus/anti-malware program on your device (and update it regularly)
• Update the operating system on your mobile device as soon as new versions become available (updates often include security patches)
• Update apps on your mobile devices as soon as new versions become available
• Avoid clicking on ads on your devices (ad-blocking apps exist for Apple and Android)
• Turn off Bluetooth when you don’t need the connection
• Keep your mobile devices locked and password-protected
• Regularly backup your mobile devices when and where possible
• For Apple devices, enable location services and “Find My iPhone/iPad”; this will allow you to remotely wipe the device through Apple’s website, www.apple.com, if the device is lost or stolen.

11IP Address: An IP (Internet Protocol) address is a numerical label assigned to each device (e.g. computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.
12SSID: SSID (Service Set Identifier) is a case-sensitive, 32-alphanumeric character unique identifier attached to the header of packets sent over a WLAN.
MALWARE

Malicious Software Fights Dirty

The long-form and official name is “malicious software.” But these days, everybody knows it as malware. Whatever term you use, the reality is very harmful. Malware is simply not nice – nor are the cybercriminals who use it to launch their online attacks. A serious and persistent threat to us all these days, malware is used to steal and/or destroy your data. What’s worse, this sinister software also compromises the security and integrity of your hardware in the process. So why should you ever begin to let your guard down? Learn how to fight back now.

TIPS + TACTICS

• Install anti-virus and anti-malware software on all your computers and mobile devices – and pay close attention to any warnings you might receive
• Don’t click on unfamiliar links, and don’t visit unsavory or suspicious sites
• Be very wary of any unsolicited suspicious emails, which are often used to deliver malware attacks (via links and/or attachments)
• Be very wary of emails that instill fear – such as a “lawsuit, unpaid traffic ticket, unpaid invoice or the shutoff of services” – these emails are also aimed at getting you to click on links and/or attachments which are often used to deliver malware attacks
• Avoid file-sharing sites
• Don’t ever click on links in pop-ups
• Keep your security software, web browser, and operating systems all up-to-date
• Make sure your firewall13 is always on
• Turn all automatic updates on
• Backup all your data frequently (in case you do suffer from a malware attack)

13Firewall: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.
SOCIAL ENGINEERING

Things – and People – Aren’t Always What They Seem

The reality is that the online world is something of a virtual reality. And now more than ever, things – and people – aren’t always what they seem to be online. Sometimes, not even close. Social media sites can be incredibly valuable and enjoyable. But they can also serve as an entryway for all kinds of cybercriminals, scammers, thieves, phishers, "spear-phishers," and other online undesirables. Even if these various "social engineers" don’t steal your information, prying online eyes can learn a lot about you via social media snooping. So be careful when you’re being social.

TIPS + TACTICS

- Limit the amount of information you share on social networks
- Limit who can view your information. You can often restrict who can view your information – from “anyone or public” to just “acquaintances or friends”
- Be extremely wary of fake profiles and people who try to connect with you on social networks
- Be on the lookout for phishing attempts (attachments, payment instructions to a new address, directives to change your password, etc.) Never click these links, rather go directly to the website and perform the action from within the website.
- Recognize fraudulent email warning signs (poor spelling, poor grammar, urgent or odd language, vague or unusual addresses)
- Keep all your security software up-to-date
- If you think any of your accounts have been compromised, change your passwords immediately (see our first section for more password tips)
- Avoid using the same password you use for social media websites on your online banking website
- If you think your online banking account has been compromised, check for unknown charges, and contact your financial institution

14Spear-phishing: Spear-phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by “random hackers” but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.
SECURE YOUR CREDIT

Utilize Credit Monitoring + Freezes

There’s no denying the importance of your credit history in today’s world. The relative strength or weakness of your credit history can determine your ability to secure loans and insurance policies, gain employment, and open credit card and bank accounts. With so much on the line when it comes to your credit, it’s vital to do everything you can to protect your credit, starting with your credit report. Each of the three major U.S. credit bureaus provides tools to help minimize the risk of your credit report being used by unauthorized entities or individuals.

TIPS + TACTICS:

- **Monitor Your Credit:** Monitoring your credit report is the best way to spot signs of identity theft, such as suspicious activity and accounts or addresses you’re not familiar with. The three U.S. credit bureaus are required by law to provide one free credit report per year upon request. Any suspicious or fraudulent credit listing you see should be reported to the credit bureau that shows the activity.

- **Implement a Credit Freeze:** Also known as a security freeze, a credit freeze restricts access to your credit report – making it more difficult for identity thieves to open accounts in your name and/or abuse your credit. A credit freeze prevents a person, merchant, or institution from making an inquiry about your credit report – unless you lift or remove the freeze. Your credit report will continue to be accessible to your existing creditors and/or debt collectors. Putting a credit freeze in place must be done individually with each of the three U.S. credit bureaus.

- **Lift a Credit Freeze:** A credit freeze remains in place until you direct the credit bureau to either temporarily lift it or remove it in full. Similar to implementing a credit freeze, each bureau may charge a fee to “unfreeze” your credit. It can also take up to three days for a bureau to act on your request to lift a credit freeze.

Request your free annual credit report at: www.annualcreditreport.com
877.322.8228
IDENTITY THEFT

Don’t Let Identity Thieves Run Free

Identity theft is no laughing matter. And more and more, it’s not just something that happens to someone else, somewhere else. To combat this rising form of crime – and safeguard and secure your own person and peace of mind – you should always pay close attention to your bank statements, credit card bills, and overall activity on all your accounts. If you do think you’ve been compromised by an identity theft, you can contact one of the three U.S. credit bureaus, and place a fraud alert on your credit file. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name – although they may not prevent any misuse of any of your existing accounts or cards. Fraud alerts do not freeze your credit, and they allow your credit score to change even as they mitigate the risk of unauthorized use.

TIPS + TACTICS

Three types of fraud alerts:

• **Initial Fraud Alert**: Primarily designed for individuals who feel their identity has been compromised. Initial Fraud Alerts last 90 days from the date issued, can be continuously renewed, and are entirely free of charge to you.

• **Extended Fraud Alert**: Reserved exclusively for victims of identity theft, Extended Fraud Alerts are designed to protect your credit for seven years.

• **Active Duty Military Alert**: Reserved for military personnel who want to protect their credit during deployment. Active Duty Military Alerts last for one year, and can be renewed.

DON’T WASTE A MOMENT

Alert Credit Bureaus Immediately

If you’ve been the victim of identity theft of any kind, it’s important to act immediately. Don’t delay. Don’t waste time worrying or wondering about all the details of the crime. Contact one of the three credit bureaus – right away. Tell them you need to place a fraud alert. Here’s how to reach them right now:

• **Experian**
  
  [www.experian.com/fraudalert](http://www.experian.com/fraudalert)
  
  888.397.3742

• **Equifax**
  
  [www.equifax.com/creditreportassistance](http://www.equifax.com/creditreportassistance)
  
  800.349.9960

• **Transunion**
  
  [www.transunion.com/fraud](http://www.transunion.com/fraud)
  
  800.349.9960
CYBERSECURITY DOs and DON’Ts


In today’s fast-moving, ever-evolving day and age, time is always at a premium. In this spirit, we offer you the following quick-hit lists to consult – whenever and wherever you may find yourself in need of a helping hand.

FIVE TOP ONLINE SAFETY + SECURITY DOs

1. Use anti-virus software, and be sure to keep it up-to-date
2. Create strong passwords, and change them every 90 days
3. Create separate email accounts for work, personal use, and other interests
4. Set up a primary network at home, and another network for guests
5. Only use an unsecured, public network when absolutely necessary

FIVE TOP ONLINE SAFETY + SECURITY DON’Ts

1. Never click on a link in an email before you validate the source
2. Never disclose personal information in an email, IM or text message
3. Never use the same password for multiple accounts
4. Never divulge sensitive information via social media
5. Never use an unsecured, public network to conduct business

FIVE INFECTED COMPUTER WARNING SIGNS

1. Noticeable change in overall performance
2. Noticeable change in screen appearance
3. Random rebooting, restarting, or lockup
4. Appearance of unusual pop-up messages
5. Unexpected toolbars or icons on desktop or in browser

FIVE HELPFUL ONLINE SECURITY RESOURCES

1. FTC OnGuardOnline  
   www.onguardonline.gov
2. FCC Cybersecurity for Small Business  
   www.fcc.gov/general/cybersecurity-small-business
3. FBI Internet Crime Complaint Center  
   www.iC3.gov
4. Microsoft Secure  
5. Pacific Premier Bank Cyberthreat Center  
   www.ppbi.com/cybersecurity
TECH SPEAK GLOSSARY
A Closer Look at Some Tech-ier Terms

It’s called “tech-speak” for a reason – because some of the truly technical terms in the tech world can appear almost like a foreign language to the untrained eye. Here at Pacific Premier Bank, we pride ourselves on our ability to connect and talk – in ways that everyone can easily understand and relate to. The following is an alphabetized collection of the footnoted terms provided throughout this document.

**Algorithm:** A process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

**Cache:** Portion of a computer’s hard disk space where a browser temporarily stores recently visited webpages to speed up internet surfing.

**Cookie:** A small file created by a website that is stored in the user’s computer either temporarily for that session only or permanently on the hard disk (persistent cookie). Cookies provide a way for the website to recognize you and keep track of your preferences.

**Encryption:** The translation of data into a secret code. Encryption is the most effective way to achieve data security by scrambling the contents into an unreadable form. To read an encrypted file, you must have access to a secret key or password that enables you to read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

**Firewall:** A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

**IP Address:** An IP (Internet Protocol) address is a numerical label assigned to each device (e.g. computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Think of your home address. It has a number, street name, etc. to help identify where your house is located. An IP address tells the internet or your home network where your computer is.

**Malware:** An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

**Phishing:** The activity of defrauding an online account holder of financial information by posing as a legitimate company.

**Social engineering:** A cyberattack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

**Software Vulnerability:** A security flaw, glitch, or weakness found in software or in an operating system (OS) that can lead to security concerns.

**Spear-phishing:** An e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

**SSID:** SSID (Service Set Identifier) is a case-sensitive, 32-alphanumeric character unique identifier attached to the header of packets sent over a wireless network.

**Two-Factor Authentication:** A method of confirming a user’s claimed identity by utilizing a combination of two different components.

**Virtual Private Network (VPN):** A private network that extends across a public network or internet. It creates an additional layer of security over an insecure network when the network infrastructure alone cannot provide it.
LET’S TALK® MORE

Exceed Your Banking Needs

We hope you found this cybersecurity guide informative and helpful. All of us here at Pacific Premier Bank remain devoted to safeguarding and ensuring your security while banking with us. We also welcome the opportunity to talk to you about meeting and exceeding any and all business and personal banking needs you may have. Drop us a line today. Let’s Talk®.

Phone: 1.888.388.5433   Web: ppbi.com/cybersecurity