Cybersecurity at a Glance

A Brief Guide to Serious Security

PACIFIC PREMIER BANK®

Protecting you is always part of what we do.

At 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 robust cybersecurity protection.

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. According to *Symantec's 2018 Internet Security Threat Report*, there are now more than 8,700 software vulnerabilities disclosed each year and the number of organizations affected by targeted attacks increased by 10 percent in 2017.

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. As we continue to expand and evolve in our fourth decade of operation, we are more devoted than ever before to staying ahead of threats to our clients' information and privacy. Let's Talk® about cybersecurity.

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 armed with robust data dictionaries, and dictionaries of words – in both English and other foreign languages. Hacker's 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.

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 as your password
- 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
- Always go to the website directly and change your password via the website. Never go through an email weblink, as the email could be fraudulent

EMAIL providers can't guarantee your security when you sign up for their services. Hackers know this and 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.

Follow these tips and don't let them get you.

- 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 online banking website
- Use data encryption to transmit personal information. Look for a padlock icon next to the website's URL in your browser window (indicating a secure connection)"
- Never send sensitive personal information (i.e. Social Security Number) over email
- Only access email accounts from secure networks; avoid access from public Wi-Fi hotspots
- Beware of unsolicited email; hackers can pretend to be anyone! Always verify with the sender before opening an attachment or clicking a link

THE WEB is a complex network that's utilized by just about anyone and everyone. Every device on the internet can be hacked – many with just minimal effort. Many cybercriminals create "clones" of well-known websites, then use them to capture user information and credentials.

Don't crash online. Drive safe.

- Keep your computer software up-to-date
- 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 connection)
- Block ads and pop-ups, and never respond to pop-ups requesting information
- Never download anything from unknown sources/websites
- Always log out after doing any online banking (be sure to end/close each session)

MOBILE DEVICES are a crucial part of our work and personal lives today. But just how secure from cyberattacks are your smartphones, tablets, and other mobile devices? Especially if they're loaded up with social networks and other assorted apps?

From Apple iOS to Android, play it safe whenever you can – and wherever you go.

- 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 trusted apps on your mobile devices as soon as new versions become available
- Keep your mobile devices locked and password-protected
- For Apple devices, enable location services and "Find My iPhone/iPad"; this will allow you to remotely wipe the device if it is lost or stolen.

MALWARE is used by cybercriminals to launch their online attacks. A serious and persistent threat is malware 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.

Malware – fight back.

- 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)
- 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

SOCIAL ENGINEERING refers to the psychological manipulation of people into performing actions or divulging confidential information for the purpose of information gathering, fraud, or system access. It is often one of many steps in a more intricate fraud scheme.

Social engineering also bends into the dark side of social media, and many popular social media sites can serve as an entryway for cybercriminals, scammers, thieves, phishers, and spearfishers. Even if these "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.

- Limit the amount of information you share and the people you become friends with
- Limit who can view your information. You can often restrict who can view your information – from "anyone or public" to just "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 or app.
- Recognize fraudulent email warning signs (poor spelling, poor grammar, urgent or odd language, vague, or weird addresses)
- If you think any of your accounts have been compromised, change your passwords right away
- 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

LET'S TALK®

Meet Your Business Banking Needs

All of us here at Pacific Premier Bank remain devoted to safeguarding and ensuring your security while banking with us. Drop us a line today. Let's Talk® about your business and how we can help you succeed.

Phone: 888.414.0515 **Web:** ppbi.com/cybersecurity

Member FDIC