# Cybersecurity Matters:

## An In-Depth Look at Online Security

PACIFIC PREMIER BANK®

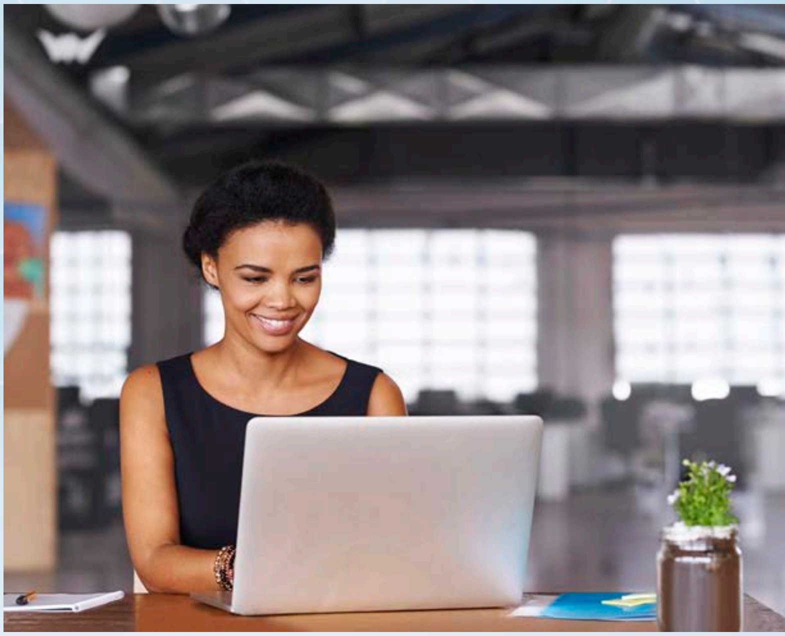
# Your Security Matters Most

At Pacific Premier Bank, we're committed to providing every client 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 to staying ahead of all threats to our clients' online accounts and privacy.

Cybersecurity threats continue to grow and evolve in their complexity, creativity, and reach. In fact, cybercrime is the world's largest criminal growth industry, costing the world $6 trillion annually by 2021.

Symantec estimates there will be 200 billion connected devices worldwide in 2020, which is incredibly concerning given a study by the University of Maryland that finds cyberattacks occurring every 39 seconds. In short, our determined efforts to recognize and prevent cyberattacks must be greater and more aggressive than those who intend to profit from them.

The good news is that information and tools exist to significantly limit the vulnerability to cybercrime. Please review this in-depth look at online security and prepare yourself to be part of the cybersecurity solution.



## Inside

Cybersecurity 1
Passwords 2
Email 3
Internet 4
Wi-Fi Hotspots 5
Home Networks/Mobile Security 6
Malware 7
Social Media 8
Secure Your Credit 9
Identity Theft 10
Dont't Waste a Moment 10
Cybersecurity DOs and DON'Ts 11
Tech Speak Glossary 12
Let's Talk® More 13

# Pacific Premier Is Here to Help

## ONLINE. ON GUARD. 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, raising 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, PPBI.com, supports SHA256, a strong encryption[1] hashing algorithm[2] technology. 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.

This informative, instructional, and helpful guide is devoted to those efforts and steps towards online safety. It identifies and illuminates several distinct areas of potential online vulnerability—and provides you with helpful tips on how you can best tighten up and bolt down in these areas. This way, you'll feel an added sense of security when it comes to your online assets, information, and identity.

Let's Talk® about cybersecurity.

[1] 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 format. 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.

[2] 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

In 2019, more than 4 billion records were exposed due to data breaches, with 63% of all confirmed data breaches involving weak, default, or stolen passwords. 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 English and other foreign languages. Their ever-evolving strategies and technologies can break two-thirds of all online passwords. In short, it's crucial that we be more careful and creative when creating our passwords.

### TIPS + TACTICS

- Create different passwords for every account.
- Use a Password Manager to safely record all of your accounts with their assigned passwords.
- Create passwords with at least 12 characters.
- Add complexity to your passwords with upper and lowercase letters, numbers, and symbols.
- Use a Password Generator to help you create complex passwords.
- Never use a single dictionary word for your password.
- Never use names, birthdays, phone numbers, social security numbers, or other personal information for a password.
- Use a phrase instead of a single word because longer is stronger and phrases are just as easy to remember.
- Never share your passwords.
- Always change your password directly at the site or through the app.
- Never respond to emails, texts, or phone calls asking you for your password or offering to help you change it.
- Never click on weblinks in emails that state your password has been compromised and you need to change your password using the weblink.
- Never use **remember me** or save passwords in your web browsers.
- Never use your social media logins (Facebook, Twitter, LinkedIn, Google, Office365, etc.) to access a website.
- Always log out from a website, never just closing the web browser with your login still active.
- Set up two-factor authentication on the sites that support it, like email, text, or app verification.
- Change your passwords at least four times a year and whenever you think a password was compromised, never reusing a password that you used recently.

# 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,[3] phishing,[4] social engineering,[5] 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.).
- Create strong passwords by following the guidelines from the previous section on Passwords.
- Avoid using the same password you use for email accounts on your banking website or any other site.
- Avoid opening or responding to emails from external, unknown, unexpected, or suspicious originators.
- Avoid opening email attachments that are unknown, unexpected, or suspicious.
- Avoid opening or responding to emails that contain spelling and grammar errors.
- Avoid opening or responding to emails that require an urgent response, threaten harm, and/or ask you to click on a link.
- Use your mouse to hover over email hyperlinks (without clicking them) to see the real URL.
- Use data encryption to transmit personal information.
- Never send sensitive personal information (i.e. a Social Security number) over email without encryption.
- Employ spam filters to reduce risk of unwanted and potentially unsafe emails.
- When available, use 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).
- In short, beware of unsolicited or suspicious emails. Hackers can pretend to be anyone! Always verify the sender before opening an attachment or clicking a link.

## 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 weblinks 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 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.

[3] 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.

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

[5] Social 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.
- Use a firewall and install antivirus and anti-malware software, always keeping them up to date.

- Back up and encrypt your computer data.
- Never use public Wi-Fi (hotels, coffee shops, etc.). If you must, use a VPN application to encrypt your connection while hiding your location and identity.
- Never share any personal or sensitive information on social media and be even more cautious with social media posts than you are with email messages because cybercriminals can use that information to phish you.
- Use only HTTPS websites ("padlock" icon at start of URL). If you must use HTTP websites, never provide any private or sensitive information.
- Never use **remember me** or save passwords in your web browsers.
- Never use your social media logins (Facebook, Twitter, LinkedIn, Google, etc.) to access another website.
- Always log out from banking and other websites, never just closing the web browser with your login still active.
- Block ads and pop-ups, and never respond to pop-ups requesting information.
- Never visit, download, or install from unknown websites.
- Keep your cookies[6] and browser cache[7] clear.
- Maintain at least a "medium-high" level of security on your browser settings.
- When available, use two-factor authentication[8] (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.
- Understand that millions of fake emails, fake social media users, fake Wi-Fi hotspots, fake websites, etc. are created every day, all intending to defraud internet users.
- **Report** any suspected attacks and change related passwords **immediately.**

[6] 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.

[7] Cache: Portion of a computer's hard disk space where a browser temporarily stores recently visited webpages to speed up internet surfing.

[8] Two-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. 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. Hackers even set up fake hotspots with the same name as hotels, coffee shops, and other popular businesses to masquerade as those businesses and trick people into connecting directly to them to conduct their cyberattacks. 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 assume that a Wi-Fi hotspot is legitimate or secure.
- Never use a Wi-Fi hotspot for shopping or banking.
- Always log out from websites, never just closing the web browser with your login still active.
- Use only HTTPS websites. If you must use HTTP websites, never provide any private or sensitive information.
- Do not allow automatic connections to non-preferred networks. Computers, tablets, and smartphones can have this setting enabled, please be sure to disable it.
- If you must use Wi-Fi for banking and other websites, use a Virtual Private Network (VPN)[9] 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).

[9] 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,[10] 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 multilayered protection in place by changing your router's name/SSID,[11] 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

- Disable location sharing and auto Bluetooth connectivity.
- 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.
- Only install mobile apps and updates from the App Store or Google Play, avoiding malicious apps, repackaged legitimate apps, and fake security apps from rogue sites that often contain malware or ransomware.
- 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 aren't using it.
- Keep your mobile devices locked and password-protected.
- Regularly back up your mobile devices.
- 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.

[10] 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.

[11] Service Set Identifier (SSID): 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 antivirus 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.
- Only install applications and updates from original manufacturer websites, avoiding rogue websites offering malicious apps, repackaged legitimate apps, and fake security apps that often contain malware or ransomware.
- 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.
- 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 firewall[13] is always on.
- Turn all automatic updates on.
- Back up all your data frequently (in case you do suffer from a malware attack).

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

## SOCIAL MEDIA

### 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. Social media sites can be incredibly valuable and enjoyable. But they can also serve as a gateway for all kinds of cybercriminals, scammers, thieves, phishers, "spear-phishers,"[13] and other online undesirables. Even if these various "social engineers" don't steal 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.

[13] Spear-phishing: An email 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:

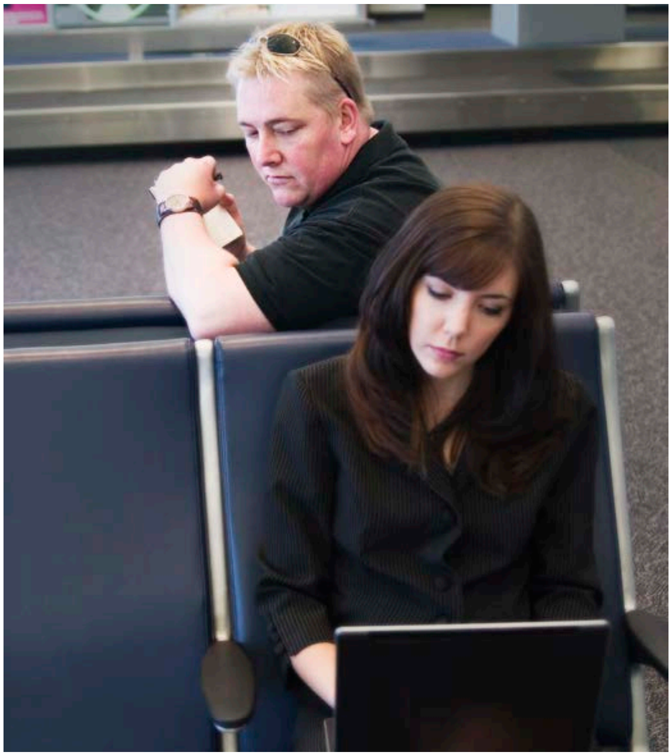
- **Monitor Your Credit:** Monitoring your credit report is the best way to spot signs of identity theft, such as suspicious activity and accounts or addresses you're not familiar with. The three U.S. credit bureaus are required by law to provide one free credit report per year upon request. Any suspicious 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 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
  888.397.3742
- **Equifax**
  www.equifax.com/creditreportassistance
  800.349.9960
- **Transunion**
  www.transunion.com/fraud
  800.349.9960

## CYBERSECURITY DOs and DON'Ts

### Stay Agile. Keep Security Simple.

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. Keep the OS, antivirus, anti-malware, web browsers, and apps on your devices up to date.
2. Create different passwords of at least 12 characters for every account and use a Password Manager to safely record all of your accounts and their passwords.
3. Back up and encrypt the data on your devices.
4. Set up two-factor authentication on sites that support it.
5. If an account gets compromised, immediately change your password and contact the business.

### FIVE TOP ONLINE SAFETY + SECURITY DON'Ts

1. **Never** click on a link in an email, social media post, or web browser pop-up before you validate the source.
2. **Never** share personal or sensitive information on social media, in an email, or via text message.
3. **Never** use **remember me** or save passwords in your web browser, or use your social media logins (Facebook, Twitter, LinkedIn, Google, Office365, etc.) to access other websites because all are incredibly insecure.
4. **Never** use a Wi-Fi hotspot, as most are very insecure.
5. **Never** install applications or updates from unknown or illegitimate websites or sources, avoiding malicious apps, repackaged legitimate apps, and/or fake security apps that often contain malware or ransomware.

### 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 Security
   www.microsoft.com/en-us/security
5. Pacific Premier Bank Cybersecurity 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, 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 format. 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.

**Spear-phishing:** An email 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.

**Service Set Identifier (SSID):** 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:** 855.343.4070 **Web:** PPBI.com/cybersecurity

EQUAL HOUSING OPPORTUNITY

Member FDIC

**Phone:** 855.343.4070 **Web:** PPBI.com

PACIFIC PREMIER BANK®