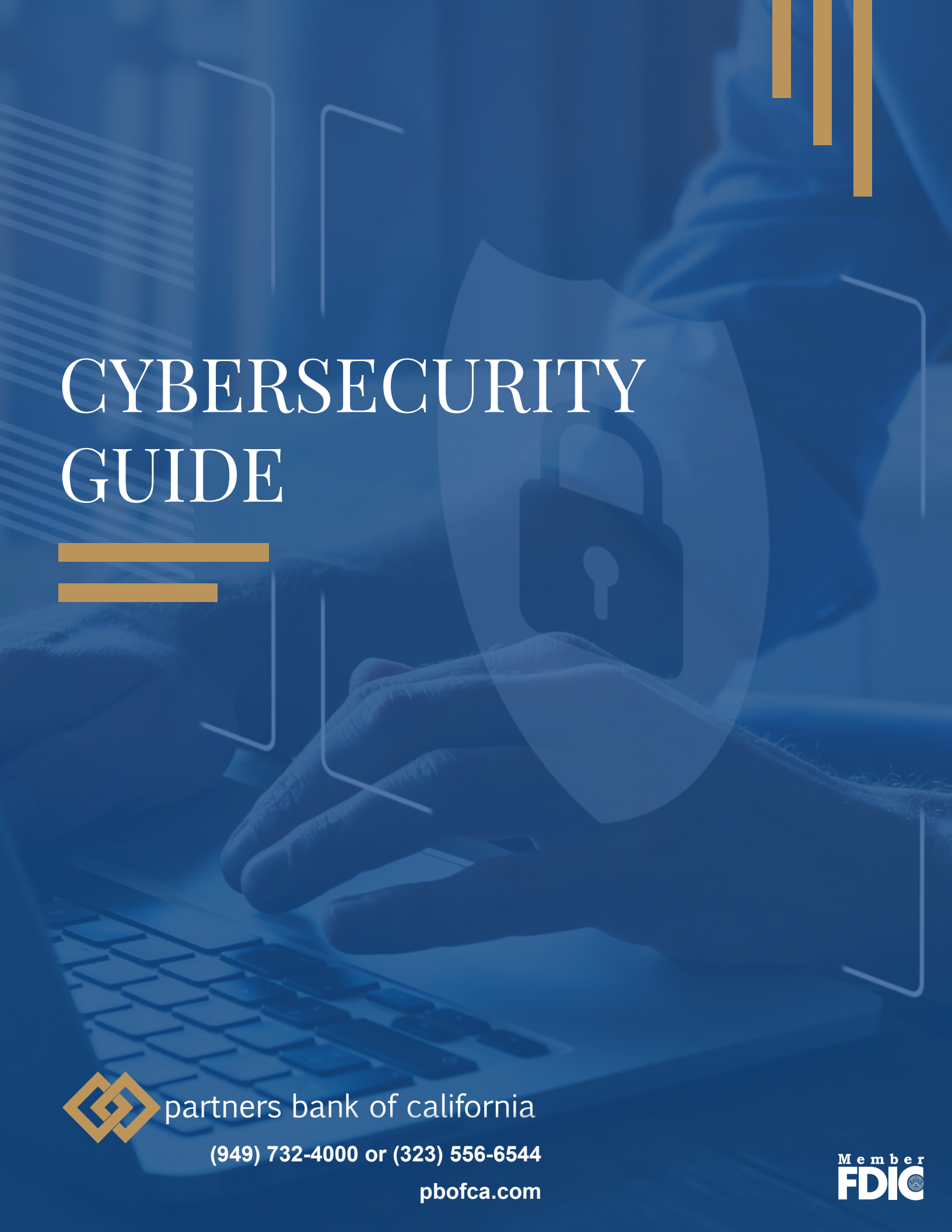

CYBERSECURITY GUIDE

partners bank of california

(949) 732-4000 or (323) 556-6544

pbofca.com

10 WAYS TO PROTECT YOUR PERSONAL INFORMATION & DATA

With scammers, hackers, and other bad guys trying to steal your personal information online, it's a good idea to know how to lock down your devices, network, and information. That way, your passwords, Social Security number, or account numbers are protected from scammers. Check out these tips from the Federal Trade Commission (FTC) to protect your personal information and data.

SECURE YOUR DEVICES

1. Keep your security software up to date.

Your antivirus or firewall programs must be up to date to work, whether they came pre-installed or you loaded them onto your device.

2. Be sure to update your operating system software.

This could be Windows, Apple OS, or Chrome, for example.

3. Keep your internet browsers and apps up to date.

Developers often provide updates to address security issues, to fix bugs, or add new features.

SECURE YOUR DATA

4. Back up your data to protect it.

Backing up your data means making an extra copy of all your files. That way, if something happens — say a virus, your device crashes, or you're hacked — you still have your files. It's important to do it once a week so you don't lose important data, like your photos, documents, and files. If you do need to restore a backup, it will only be as current as the last time you backed up. Here are two options, and a few things to consider when choosing how to back up your files:

- **Save your files in the cloud.** There are many cloud storage services that let you save files and data online. You may be familiar with some, like Google Drive, Evernote, Dropbox, OneDrive, or iCloud, but there are many others out there. Many of these services come with some free storage space, and you can pay for more storage. When you save your information in the cloud, you're trusting someone else to keep that information safe. If you're thinking about using cloud storage, find out what level of privacy or security the different services offer.

- **Save your files to an external storage device.** A USB flash drive is an affordable option that offers a moderate amount of storage. Another option is an external hard drive. It might cost a little more than a USB drive, but it can give you more storage capacity, transfer data faster, and be more reliable. You can decide which files or folders to back up, and you may be able to schedule automatic backups.

SECURE YOUR ACCOUNTS

5. Create and use strong passwords.

That means at least 12 characters. Making a password longer is generally the easiest way to increase its strength. Consider using a passphrase of random words so that your password is more memorable, but avoid using common words or phrases.

6. Use multi-factor authentication.

Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

7. Choose security questions only you know the answer to.

Many security questions ask for answers to information available in public records or online. So, when you can, avoid questions like your zip code, mother's maiden name, and birth place. And avoid using questions with a limited number of responses that attackers can easily guess — like the color of your first car. You can even put in random answers to make guessing more difficult.

BE MINDFUL OF PEER-TO-PEER FILE SHARING

8. Scan files before you open them.

If you decide to use a peer-to-peer program, use your security software to scan any files before you open them, and before you play any downloaded files. Avoid any peer-to-peer program that asks you to disable or change the settings of your firewall. Disabling or changing these settings could weaken your computer's security.

PROTECT YOUR HOME NETWORK & YOURSELF WHILE ON WI-FI

9. Secure your home network.

One important way to protect your information is to protect your network at home. Think of your router as the connecting point between your devices and the internet. If malware gets onto any of your connected devices, it can spread to the other devices connected to your network. Your devices, accounts, and whole network are only as secure as your router.

10. Protect your personal information while you're online.

You can control how secure your home network is — but you can't do the same for public Wi-Fi. It's always best to assume it's not secure. Save your online shopping, banking, and other personal transactions for when you're on your home network. Or use your mobile data, as that data is typically encrypted.

REPORT IDENTITY THEFT

If you think someone has gotten into your accounts or has your personal information, visit IdentityTheft.org. There, you'll get steps to take to find out if your identity has been misused, and how to report and recover from identity theft.

WE'RE HERE TO HELP

Your online safety and financial health are very important to us. For more information and resources regarding online safety and security, please visit pbofca.com.

If you have any questions or need assistance regarding online banking or any of our products and services, please give us a call at (949) 732-4000 or (323) 556-6544, or email us at onlinebanking@pbofca.com