Is Your Information Secure?

A GUIDE TO CYBERSECURITY

Central Valley Community Bank

www.cvcb.com

Is Your Information Secure?

A Guide to Cybersecurity

Central Valley Community Bank

At Central Valley Community Bank, your security is our top priority.

Protecting your business and personal identity online, at home, or out-and-about requires ongoing education and daily effort to thwart the negative impact of cybercriminals. Central Valley Community Bank provides extensive safeguards to secure our customers' financial relationships and is committed to offering education and helpful resources to help protect your business and personal information both online and off.

This Q&A includes helpful tips and information on how you can protect what matters most to you and your business.

The Threats Of Cybercrime

1. What is cybercrime?

Cybercrime is a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device.

2. What are the most common ways that cybercrimes can occur?

Some examples of cybercrimes include:

Computer or network intrusions
Cybercriminals gain access to devices and networks through email or the internet. These attacks aren't necessarily meant to steal information, but rather cripple your computer or network, forcing very expensive repairs and business delays.

"Spam" or deceptive emails
Spam or deceptive emails look so real that users tend to "click" on links without thinking. Unfortunately, these emails contain spyware and clicking or sometimes even simply opening the email opens a window for fraudsters to gather your personal or business information and use it for fraudulent purposes.

Ransomware
An insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. The FBI doesn't support or recommend paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization will get its data back.

Phishing
Occurs when someone posing as a trusted advisor uses fake emails, texts, or even phone calls to trick you into sharing valuable personal information, like account numbers, Social Security numbers, or your login IDs and passwords.

Cellphone takeover
When the operating system of your cellphone and all associated apps are compromised.

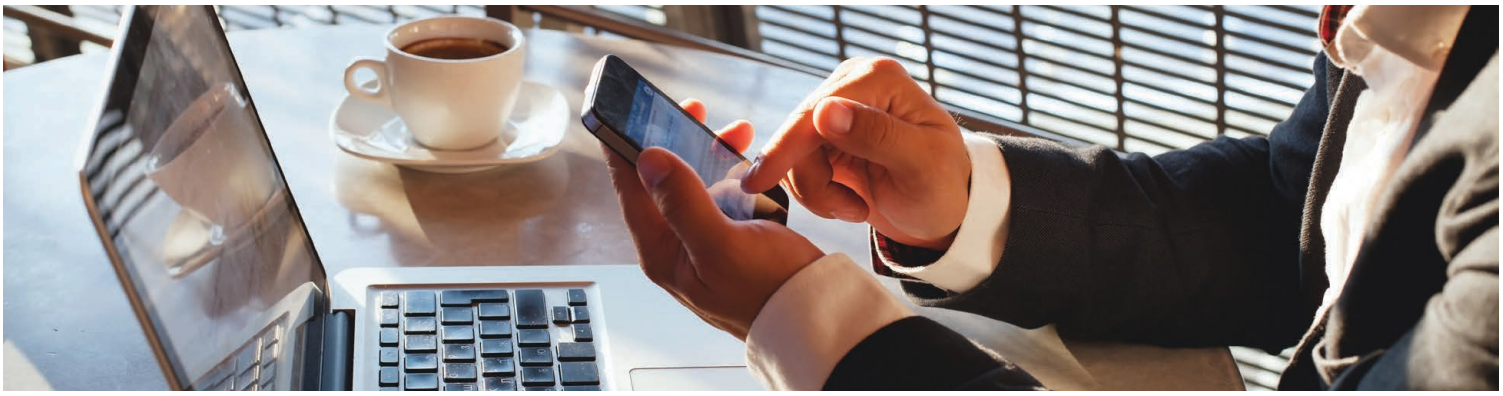
3. How can I protect myself online?

The best rule of thumb is to "think before you click" on websites and emails. Cybercriminals are very good at making fraudulent websites and emails look like regular communication from your favorite brands.

When making a transaction online, be sure it is over a secure, encrypted site. A "lock" icon on the status bar of your browser means your information is safe when transmitted. It is also a good idea to add two-step verification to all online shopping and credit card accounts when available.

Password-protect your mobile and desktop devices. Create and regularly update passwords that mix letters, numbers and special characters. Do not store passwords on any device or in your email. Set your phone and computer to automatically lock when not in use.

Turn off and don't establish connections with open Wi-Fi networks when you are at public establishments. Coffee shops and restaurants are common places that cybercriminals hang out and hack into accounts.



Protecting Yourself From Cybercrime:

Preventing Identity Theft

4. What is identity theft?

Identity theft is a type of cybercrime in which someone wrongfully obtains another individual's personal information and then uses it for their own economic gain.

5. How prevalent is identity theft and fraud?

According to the 2019 Identity Fraud Study released by Javelin Strategy & Research, approximately 14.4 million Americans were affected by identity theft in 2018. Fortunately, this is nearly two million fewer individuals impacted in 2017 due to more public education, however the financial losses associated with these types of fraud are still staggering. Almost $15 billion dollars was stolen from victims of identity fraud.

The study also found that:

- Fraudsters are growing even more adept at overcoming authentication challenges – takeovers of mobile phone accounts nearly doubled in 2018.
- Fraudsters also have heightened their attacks on peripheral financial accounts like rewards programs and retirement accounts.
- Shopping online presents the greatest opportunity for fraud.

Additionally, the Federal Trade Commission reported that California had the third highest rate of identity theft in the U.S. in 2018.

6. What are the most common ways that identity theft can happen to me?

Cybercrimes are rapidly increasing, however, criminals are still using many simple, low-tech methods of identity theft. Some examples include:

Shoulder surfing
Nearby criminals listen and watch while you are making everyday purchases, hoping to capture your personal information.

Credit card fraud
When your credit card information falls into the wrong hands, damage can happen very quickly. The good news is that most credit cards now include a safeguard that monitors unusual activity. When suspicious activity is determined, there's a hold put on the card and it is not lifted until the user is verified as the rightful owner of that card.

Pre-approved credit cards
Everybody gets mail offers with pre-approved credit cards. These can be retrieved by criminals who attempt to activate them without your knowledge. It's important to shred and properly discard these unsolicited mailings.

Mail fraud or dumpster diving
Fraudsters literally go through your trash to gather personal information on you or your business and piece it together for fraudulent purposes. This is another reason why properly shredding documents is so important.

7. What happens when your personal or business information is obtained fraudulently?

With enough identifying information about an individual (sometimes they only need three items!) a criminal can take over your identity to conduct a wide range of crimes.

Forms of identifying information that criminals look for:

- Your full name
- Address
- Email address
- Date of birth
- Social Security number
- Credit card or bank account numbers

Once fraudsters get your information, there are many ways they can conduct crimes, such as:

- Make false applications for loans and credit cards.
- Make withdrawals from your bank accounts.
- Access and use your online accounts.
- Use your identity to obtain other goods or privileges that they might be denied if using their real name.

Preventing Identity Theft (Continued)

8. What are some of the warning signs of identity theft?

Charges for goods or services you didn't purchase appear on your credit/debit card statements - Don't ignore small charges. Thieves who use stolen account numbers sometimes do a test with a small purchase. If you didn't authorize it, check it out.

A new credit card or store charge card that you didn't apply for shows up in the mail - An ID thief pretending to be you may have applied for that card. Don't assume it's a mistake. Contact the company right away.

Statements show up for an unknown credit card account - Armed with the right information, thieves can apply for credit cards in your name and go on a shopping spree before the crime is discovered and the account is closed.

Missing mail or email - There could be a problem if the monthly statement from your bank or credit card company suddenly stops. A thief may have filed a change of address form to get that statement and keep you from spotting their crime for as long as possible.

Collection notices or calls for a debt you don't owe - It could be an honest mistake or it could be that a thief is using your personal information to buy things and not pay the bill.

Errors (misinformation) on your credit report - You have the right to a free report every 12 months from the big three credit bureaus (Experian, Equifax, and TransUnion). Get a report from one of the bureaus every four months and look for anything suspicious, such as an account you didn't open or credit inquiries when you didn't apply for credit. Use this site: **www.annualcreditreport.com.**

You have good credit, but your application for new credit is denied - Don't get upset and find out what's going on. An identity thief could have ruined your credit score.

9. How does identity theft impact your credit score?

In most cases, a fraudster takes out a credit card in your name, maxes out the card and payments are never made. And although every credit inquiry could take 10 to 20 points off your score, the increase in credit card debt will hurt your score even more.

Missed payments will have the biggest impact. You could easily lose more than 100 points as a result of a fraudster's activities until you take the steps to notify the credit reporting agencies and clean up your report.

10. How can I protect myself from identity theft?

Education is the first step in protecting yourself from identity theft. Be aware of current schemes fraudsters are using to obtain your personal information.

Shred sensitive documents that you don't need anymore. Tax records should be kept for 7 years after consulting with your tax advisor. After that, professionally shred the old ones. While personal shredders help, professional shredding companies are able to shred documents in a way that make it nearly impossible to patch back together for fraudulent purposes. Central Valley Community Bank offers free shred events in the spring. For more details, please see page 6.

Regularly review your bank and credit account billing statements to make sure there are no suspicious purchases, as well as annually reviewing your credit reports. You can obtain a free credit report annually from each of the three nationwide reporting companies (Equifax, Experian, TransUnion) at **www.annualcreditreport.com** or by calling (877) 322-8228.

Protect your personal information. Don't give it to anyone unless you are sure who they are and what they are using it for. This includes Social Security and PIN numbers, which should be memorized instead of carrying with you.

You should also change PIN numbers and online passwords periodically, and use a combination of letters and numbers when creating them.

11. What steps should victims of identity fraud take to report the crime?

Immediate action on your part is needed to reduce the degree of impact caused by fraudulent use of your identity. If you are a victim of identity fraud you should:

- Immediately report this to your bank and credit card issuers.
- File a police report and call the fraud unit of the three credit reporting agencies

TransUnion (800) 680-7289 | Experian (888) 397-3742 | Equifax (800) 525-6285

- Download the Federal Trade Commission's Identity Theft Recovery Plan at **www.IdentityTheft.gov**.
- Consider identity theft protection like LifeLock or Experian.

Protecting Your Business From Cybercrime

12. How are businesses affected by cybercrime?

Businesses can often be a victim of a targeted cyberattack, which is an effort to penetrate acompany's network defenses and either cause damage or extract high-value assets and processes from within an organization.

To thwart such attacks a business must be cyber-resilient. A cyber-resilient business must have cybersecurity policies, business continuity plans and enterprise resilience initiatives in place. These security strategies allow the business to respond quickly to threats, so it can minimize the damage and continue to operate.

As a result, the cyber-resilient business can introduce innovative offerings and business models securely, strengthen customer trust, and grow with confidence.

13. How can a business become cyber-resilient?

As organizations invest in digital technology to keep pace with competition, they also need to keep up with cybersecurity measures. Though certain commonly used business software programs and cybersecurity measures provide everyday defense against attacks, the cybercriminals are advancing their attack strategies every day. Information technology consultants can be engaged to provide network "health assessments," such as penetration tests or vulnerability assessments.

Top-down education for all employees is also a must. Specialty risk management firms can be contracted to conduct tests and network security audits for both technology systems and for human resources procedures. The purpose of these human resources security audits is to test employee knowledge with established security procedures surrounding phone, internet and email-based communications. It's not uncommon for businesses to find themselves well below the standards of security when these tests are administered.

Focused training programs to make employees more aware of cybersecurity risks, procedures and controls can help detect and prevent these risks from being exploited by the criminals. HR policies can also be implemented to help monitor employee risk levels and offer additional training for those who don't pass simulations.

14. How important is it for a business to invest in cybersecurity measures?

The impact of a cybercrime to a business ranges from negligible to catastrophic. It can create complete paralysis and destruction of systems and infrastructure or it might only impact non-critical functions with intermittent interference. Regardless of the effect, business interruptions and cyber breaches can create huge reputation and cost risks to a business, which is why cyber insurance is important for all businesses to add to their suite of protection elements.

15. Should a business invest in cyber risk insurance?

Whether your business is small or large, there are cyber policies available through your current insurance broker. These policies can help defray the costs associated with restoring a business back to health in the event of a cybercrime.

16. Should a business regularly shred documents?

As with individuals, businesses should regularly shred documents. Document shredding companies have mobile shred trucks that come directly to your place of work and shred unneeded paperwork, if you don't already have that in place.

Central Valley Community Bank offers free shred events in the spring. For more details, please see page 6.

How Banks Are Protecting Their Customers

17. How do banks help customers with concerns about identity theft?

Banks have dedicated departments with highly trained employees who are equipped to assist with fraud of all types. They are experienced in investigations and in working with the authorities and are committed to resolving issues for customers no matter how long it takes – in some cases it can take years to rectify the damage a fraudster can cause.

In addition, banks offer cybersecurity training, whether in a physical setting or online through their websites. It is highly recommended that all businesses seek training programs for their entire team. According to experts, it's typically an employee of a business who unknowingly clicks on a fraudulent email or answers a fraudulent call that opens the door to trouble. The FDIC offers "A Cybersecurity Guide for Business" which is a great tool for businesses to have as a reference.

18. How do banks respond when contacted regarding fraud?

Once you contact your bank about possible fraud, it immediately takes action by beginning an investigation and closing accounts when appropriate. Many banks have special toll-free numbers devoted to helping victims of identity theft.

Many banks also offer worksheets and standardized affidavits for you to send to other businesses that may need to be contacted about the fraud. One affidavit that is a valued resource is the Federal Trade Commission's Identity Theft Recovery Plan at **www.ftc.gov/idtheft**.

19. What should we know about how our banks are helping to protect customers and the community?

Data security is a top priority for banks and we have the highest level of security among critical industries. A regulatory system is already in place and banks are routinely examined by the government to ensure their computer systems are robust and in compliance with the law to ensure the customers' information is safe and secure.

Central Valley Community Bank takes measures to protect its customers by:

- **Providing educational programs including:**
  - Seminars for businesses and individuals.
  - Programs offered in the classroom at local colleges and high schools.
  - Public service programs where local media and social platforms are used to share messaging on the subject and resources for help.
- **Offering products and services that include identity protection features**
- **Protecting consumers against losses. When a customer reports an unauthorized transaction, the bank covers the loss and takes measures to protect your account (customer liability limited to $50)**
- **Offering zero-liability fraud protection so most victims don't experience any out of pocket costs**
- **Continuous engagement with law enforcement daily to manage new risks being detected, in addition to supporting issues for customers**
- **Partnerships with local, state and federal agencies to develop awareness programs to protect banks and their customers from this issue**
- **Annual Shred Events (free up to four banker boxes)**

Central Valley Community Bank recommends shredding important documents regularly as one easy step to help prevent becoming a victim of identity theft and fraud.

Annual Document Shredding events (up to four banker boxes) take place every spring at CVCB branches across the Central Valley and Greater Sacramento. Additional information can be found on the Bank's website at **www.cvcb.com/shredding**.

Helpful Resources

Learn more about identity protection and cybersecurity by visiting the following websites

Federal Trade Commission
www.ftc.gov

United States Computer Emergency Readiness Team
www.us-cert.gov

Federal Deposit Insurance Corporation
www.fdic.gov

Internal Revenue Service
www.irs.gov