



CYBERSECURITY FOR SMALL BUSINESS

Vendor Security





Your Business Vendors May Have Access to Sensitive Information

Make sure those vendors are securing their own computers and networks. For example, what if your accountant, who has all your financial data, loses his laptop? Or a vendor whose network is connected to yours gets hacked? The result: your business data and your customers' personal information may end up in the wrong hands — putting your business and your customers at risk.

How To Monitor Your Vendors



Put it in writing

Include provisions for security in your vendor contracts, like a plan to evaluate and update security controls, since threats change. Make the security provisions that are critical to your company non-negotiable.



Verify compliance

Establish processes so you can confirm that vendors follow your rules. Don't just take their word for it.



Make changes as needed

Cybersecurity threats change rapidly. Make sure your vendors keep their security up to date.

How To Protect Your Business



Control access

Put controls on databases with sensitive information. Limit access to a need-to-know basis, and only for the amount of time a vendor needs to do a job.



Safeguard your data

Use properly configured, strong encryption. This protects sensitive information as it's transferred and stored.



Secure your network

Require strong passwords: at least 12 characters with a mix of numbers, symbols, and both capital and lowercase letters. Never reuse passwords, don't share them, and limit the number of unsuccessful log-in attempts to limit password-guessing attacks.



Use multi-factor authentication

This makes vendors take additional steps beyond logging in with a password to access your network — like a temporary code on a smartphone or a key that's inserted into a computer.

What To Do If a Vendor Has a Security Breach



Contact the authorities

Report the attack right away to your local police department. If they're not familiar with investigating information compromises, contact your local FBI office.



Confirm the vendor has a fix

Make sure that the vendor fixes the vulnerabilities and ensures that your information will be safe going forward, if your business decides to continue using the vendor.



Notify customers

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft.



Interested in learning more?



For additional information on cybersecurity, including what to do if your business experiences a data breach, please visit our Resource Center on pbofca.com or contact support@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.



partners bank
of california

MISSION VIEJO

Corporate Headquarters
27201 Puerta Real, Suite 160
Mission Viejo, CA 92691

(949) 732-4000

BEVERLY HILLS

8484 Wilshire Blvd., Suite 520
Beverly Hills, CA 90211

(323) 556-6544

pbofca.com

© 2023 Partners Bank of California. All rights reserved.

