



# PROTECT YOUR BUSINESS WITH DATA **ENCRYPTION**



Even smaller enterprises shouldn't discount the value of their intellectual property like business plans, designs, formulas, and vendor lists.

No matter what industry you're in, you almost certainly handle and share sensitive data.

### **Protect Your Business with Data Encryption**



Does your firm have an up-to-date cybersecurity strategy that includes encryption?

Many entrepreneurs assume that their company isn't big enough to attract the notice of hackers – but this is a major misconception. Companies of all sizes are at risk for data breaches, and small businesses are increasingly a favorite target. And when hackers strike, the consequences can be disastrous: a recent study found that 60% of small businesses that are hacked go out of business within six months.

No matter what industry you're in, you almost certainly handle and share sensitive data – like your employees' Social Security numbers, your customers' credit card information, vendor lists, and your own bank account details. Encryption technology can limit the fallout from a

cyberattack by making this data unusable to the perpetrators, even if they manage to gain access to your devices or systems. If you haven't looked into data encryption for your company, now's the time.

### What Is Encryption?

If you've ever gotten a magic decoder ring in a cereal box or used a substitution cipher (like A = 1, B = 2, C = 3) to write a secret message to a friend, you have experience with basic data encryption.

In the computing world, highly sophisticated algorithms are used to convert plain text into cipher text that requires a unique key to read. You can encrypt individual pieces of information, whole files, or an entire hard drive. To any unauthorized user, the data will just look like a random jumble of characters. For example, here's what a credit card number looks like once it's been encrypted with an NSA-approved cipher:

*sW74ZRqauNuJYX0DbVe723i0rUKyLklyxrqsD70G8qmGpXPfjdSmbn8qUPSbFyB7IY54VZJHpXVYuqxz2SQwKTeM+ihk/wDJKI8z5wuZHYkHlp+Z68jeL1i8G4zdafe*

Good luck to any cyberthief who tries to figure that one out! Meanwhile, by entering a password or inserting a USB device, you or any authorized user can instantly access the decoded data.

### How to Use Encryption

It's relatively easy to implement encryption across a variety of files and devices:

- **Individual computer files** can be encrypted with a variety of open source and subscription-based software programs.
- **Desktop and laptop hard drives** can be encrypted using tools that are already part of your operating system. For Windows, it's BitLocker, and for Mac, it's FileVault.
- **External hard drives and thumb drives**, aka flash drives, can also be encrypted with BitLocker or FileVault.
- **Smartphones** may now have encryption turned on by default. To confirm settings on an Android, go to Settings, then Security, then Encryption. On an iPhone, go to Settings and then Face ID & Passcode.
- **Internet traffic** can be encrypted with a VPN (virtual private network), which protects your data from interception while in transit. VPNs can be custom-built or accessed through subscription-based services.

### Why Encryption?

Here are five specific reasons that you should consider adopting data encryption technology:

1. **Limit the cost of a lost device.** If a laptop goes missing on a business trip or a smartphone is swiped off someone's desk at the office, you might have to pay to replace it. But better to lose

\$1,000 than to lose \$50,000 – which one study estimates is the average cost of a lost business device with sensitive data on it.

2. **Foil ransomware attacks:** This is a growing form of cybercrime in which important files are stolen and held for ransom – and perpetrators can demand extra by threatening to release sensitive data to the public. If your files are backed up and encrypted, you won't have to give in to extortion.
3. **Defend against corporate espionage:** While personal and financial info is most vulnerable to theft, even smaller enterprises shouldn't discount the value of their intellectual property like business plans, designs, formulas, and vendor lists. Encryption can ensure that trade secrets won't fall into your competitors' hands.
4. **Keep Your remote workers secure:** Cybercrime has kept pace with the increase in telecommuting. It's great to give your team the flexibility to work from home or on the go, but remote desktop tools and unsecured public Wi-Fi networks are an invitation to hackers. Data encryption can be a vital second line of defense.
5. **Preserve Your reputation:** Hackers can sell Social Security numbers on the dark web, put charges on credit cards, and even clean out bank accounts, but the costliest aspect of a major data breach could be the resulting PR crisis. A business that fails to protect customer and vendor data will likely lose the public's trust.

### **Stay Safe. Move Forward.**

For more strategies that can help your business to thrive, consult your financial institution.

DISCLAIMER: These training materials are intended as general guidance only and may or may not apply to a particular situation based on the circumstances. The materials do not create any legal rights or impose any legally binding requirements or obligations on Genesis Bank or the Genesis Bank Institute for Entrepreneurship. Genesis Bank and the Genesis Bank Institute for Entrepreneurship make no claims or guarantees regarding the accuracy or timeliness of this information. The content of this training material is not designed or intended to provide authoritative financial, accounting, investment, legal, or other professional advice that may be reasonably relied on by its readers. If expert assistance in any of these areas is required, readers should seek the services of a qualified professional. Reference to any specific organization, commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute an endorsement, recommendation, or preference by Genesis Bank or the Genesis Bank Institute for Entrepreneurship. Copyright © 2022 Genesis Bank. The Genesis Tree Logo is a trademark of Genesis Bank. All rights reserved.



Interested in more?  
Visit [mygenesisbank.com/GBIE](https://mygenesisbank.com/GBIE)

For more information on how you can get involved with the Institute, please reach out to **Dani Feigin** • Head of Brand Partnerships  
**E** [dfeigin@mygenesisbank.com](mailto:dfeigin@mygenesisbank.com) **P** 949.273.1497  
**A** 4675 MacArthur Court, Suite 1600 Newport Beach, CA 92660