

# Playing It Safe

*Even small businesses need cybersecurity*

## JEWELRY BUSINESS OWNERS AND

employees understand the importance of physical security. But I'm starting to think that we don't always understand the need for cybersecurity. It's not uncommon for business owners to say to me, "Why would someone cyberattack my business? It's not like I'm storing thousands of credit card numbers on my website or trading in bitcoin!"

While it's true that a cybercriminal will gain more from a successful attack on Walmart than on a small retail jeweler or manufacturer, this does not make your business cyber-safe. According to Verizon's 2018 Data Breach Security Report, 58 percent of all cyberattacks are directed

at small business.

Many cyberattacks are aimed at obtaining personal data, either for credit card theft or other types of identity theft. As large businesses have stepped up their cyber safeguards, online thieves have discovered that small businesses present a much easier target. Sure, they have to attack more of them to get the same result, but that doesn't bother cybercriminals. They just write a bit of code and let a digital robot do the work. One attack or thousands of attacks—it's all the same to the average cybercriminal.

The damage of a cyberbreach is twofold: First, the cybercriminals mess up your data and steal your information.

Second, you must disclose to your customers what happened, and you may be required to offer free identity theft screening or other similar compensation. According to the Federal Trade Commission, "Most states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In addition, depending on the types of information involved in the breach, there may be other laws or regulations that apply to your situation."

The stakes are arguably higher for a jewelry business than other types of business. Trust plays a very large part in the jewelry buyer and seller social contract, and a cyberbreach is a major breach of trust. Cyber theft won't just mess up your week—it can also damage your brand.

So what should a small business owner do to guard against a cyberattack? According to that Verizon report, 48 percent of last year's breaches were due to hacking, and 30 percent were due to malware, so you need to guard against both. That means using both technology and behavior to protect your business. The technology part is easy; the behavior part, less so. Let's take a look at the specifics.

## USE A FIREWALL

The first line of defense against cyberattacks is a firewall. But not just *a* firewall—you now need more than one. Until recently,



*As large businesses have stepped up their cyber safeguards, online thieves have discovered that small businesses present a much easier target.*





*If you don't take advantage of the software updates created by the makers of your business software, you will be vulnerable to preventable attacks.*

most small businesses considered it sufficient to have just an external firewall that protects the company computers from the external network—the internet. You need one of those for sure. But you also may need an internal firewall.

An internal firewall protects the data moving around inside your company network. Why do you need to protect that data? For two reasons. First, much white-collar crime has an inside element, making it more important than ever to control access to your data. The tools for getting around permissions and passwords are increasingly sophisticated and available, so an internal firewall is an additional line of defense. Second, consider the statistic that 30 percent of cybercrimes are due to malware. There's always someone who will open an e-mail attachment without thinking, and malware often attacks unmanned devices such as printers and routers. An internal firewall can provide some protection (not complete) against those types of incursions.

If your employees do any work for the company from home computers or personal mobile devices, it's important to have a company security policy that makes it clear that employees must protect their personal devices with firewall protection. If you require employees to work from

personal devices, then you will be doing your company a big favor by providing the firewall licenses for them to use.

Even if you manage to do most of your own computer management and administration, firewalls are your first line of defense and important enough to hire a cybersecurity expert to install, configure, and maintain.

### COMPANY SECURITY POLICY

You probably already have a physical security policy, but it should also include cyber practices. Employees are your front line for protecting your data, detecting scams and fraud, avoiding e-mail-delivery of malware, protecting customer credit cards, and quickly identifying security incidents so you can respond to them. Just like your physical security policy, a cybersecurity plan helps you identify risks, articulate your expectations, and train your employees.

The Federal Communications Commission offers CyberPlanner, a free online tool to help you create your company's security policy and keep it up to date.

### PROTECT AGAINST MALWARE

We all know that phishing is a serious threat and that we should never open an e-mail from an untrusted source. Yet 30

percent of employees who received them, opened phishing e-mails last year! Company security policies and training are an important first line of defense, but you also need anti-malware software to detect and remove malicious software before someone has a chance to activate it.

It's also important to train, test, and reinforce employee behavior around phishing. Many companies today offer phishing simulation training programs. They randomly send phishing e-mail to you and your staff. When employees open them (and they will), it gives you the opportunity to provide additional training. Most employees become much more vigilant after one such experience, so these training programs are well worth the small investment. I recommend alerting your staff that you have hired such a company. Just knowing someone will be testing and watching is enough to change e-mail behavior!

### UPDATE, UPDATE, UPDATE

Cybersecurity is the biggest reason of all to keep all your software programs up to date. Hackers and malware programmers constantly develop new ways to break into your business. The makers of your business software—including word processing and spreadsheet programs, business and accounting systems, and website platforms—have entire teams dedicated to staying one step ahead of hackers. As they identify weaknesses (or as weaknesses are exploited), they create patches and update software. If you don't take advantage of those software updates, you will be vulnerable to preventable attacks. Too many small business owners try to save money by skipping a year (or two, or



four!) of software maintenance, but the risk just isn't worth it.

### GET PICKY ABOUT PASSWORDS

PASSWORD1234 was never an acceptable password. But it's still being used, along with birthday dates, names of children all strung together, and pet names. It's easier than ever to hack passwords, and hackers can mine entire libraries of social media data to assist their password-hacking programs. One of the most important things you can do to protect your business is to insist on strong password protocols.

Of course, this starts with you.

Rather than keeping passwords in a little printed journal, or struggling to remember challenging pass-phrases, do yourself—and your business—a favor, and invest in password management software, such as LastPass, KeePass, or Dashlane. With these systems, all you need to remember is one (very challenging) password to access the password management software. The system remembers and manages the rest. A password management system will allow you to:

- Use a different, strong password for every single website and program you use.
- Share and send passwords securely, and centrally manage shared accounts.
- Instantly remove password access from someone if necessary.
- Access your software and websites even if you don't have your password book with you.
- Use your memory for more important things.

In addition, put password management policies in place. Many software programs allow you to enforce a pass-

word policy to automatically ensure that passwords are strong, changed as often as required, and not just going back-and-forth between the same two passwords over time.


### MULTIFACTOR IDENTIFICATION

Multifactor identification is a security approach that requires more than one method of authentication to log into a program. The easiest method is to have a code sent to your mobile phone. So, you must know your username and password (factor one), and then you must have the mobile device previously listed on your account profile to receive the code (factor two). The chances of a cybercriminal suc-

cessfully hacking your password *and* having your mobile device are extremely slim.

Require all employees (and yourself, of course) to use multifactor identification for accessing any program that provides the option. This is one of the best ways to keep online and e-mail accounts from getting hacked.

Online security is constantly changing, and what is considered good practice today could be outdated tomorrow. Implementing these six suggestions—and staying on top of them going forward—will significantly reduce the risk that you or your customers will be the victims of cybercrime. ♦




**Beads and Tubes**  
Extensive line  
Plain and Fancy

**Proudly made in  
the U.S.A**

**JAM**

**James A. Murphy Bead**  
50 Colorado Avenue  
Warwick, RI 02888  
401.681.4400  
[www.jambeads.com](http://www.jambeads.com)

See us at MJSA Expo Booth #400

A division of  **National Chain Group** 401.732.6200 Warwick RI, 02886 [www.natchain.com](http://www.natchain.com)

• all shapes • all sizes • all textures

Available in a wide variety of shapes and sizes in sterling silver, gold filled, 10k, 14k, 18k yellow, white, rose and pink gold, in addition to base metal.

Contact your sales representative or call us for more details