CF CYBERSECURITY GUIDE AND BEST PRACTICES

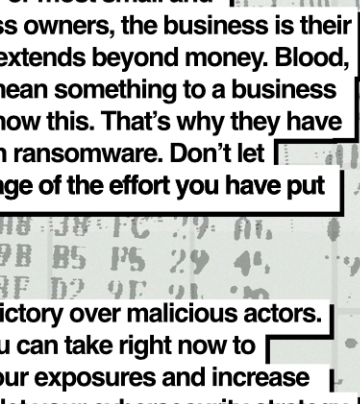
A North Korean hacker group used stolen NSA technology to infect hundreds of thousands of businesses worldwide with ransomware. The largest consumer credit reporting agency in the United States was breached, putting 145 million social security numbers in the hands of criminals. A hacker group moved from targeting medical practices to stealing student data from school districts in an attempt to threaten and extort children. This was the reality of life in 2017. This was the year that cyber attacks became mainstream.

There's no going back. Cybersecurity can no longer be considered the exclusive concern of large corporations and national governments. The criminals are too sophisticated and our reliance on technology is too absolute to ever go back to a time when this was not an essential part of our lives. We all have exposures. The question now is what are we going to do about them?

> 61% Of all cyber attacks in the US are perpetrated against small businesses.

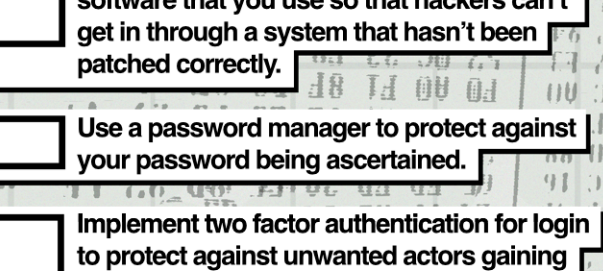
This question is especially pressing for small and medium-sized business because they are the new favorite target of cyber criminals. 61% of all cyber attacks in the US are perpetrated against small businesses. 60% of small businesses that suffer a major data loss go out of business in the next 6 months. And the numbers are only getting worse.

As a small business owner, you're on the edge of a 1,000 foot cliff. And you don't even know it.



But the fact that you're on this page means that you have taken the first step to doing something about it. Now you can start being proactive about the security of your business.

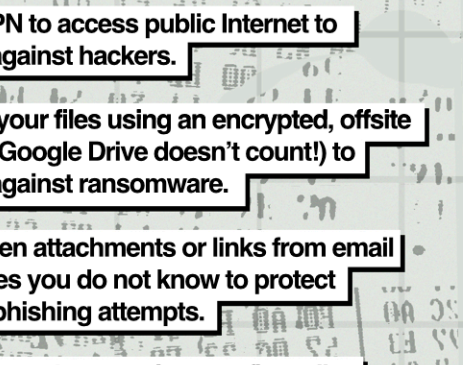
The large corporations may grab the headlines, but hackers love small and medium-sized businesses because of their lack of security measures. Now it's true that the average law firm, mom-and-pop store, or health practice doesn't store 145 million social security numbers or tens of millions of credit card numbers. But that doesn't mean that small businesses don't store valuable information. And if you have any valuable information at all, then you're a target.



But what counts as valuable information? Well, do you store any employee records, personal information of customers, health records, or credit card numbers? Is any client information on any of your computers or systems? If so, you have information that hackers want. If you're a business operating in the 21st century, you are a target.

You know what else makes you a target? Caring about your business. For most small and medium-sized business owners, the business is their entire livelihood. This extends beyond money. Blood, sweat, toil, and tears mean something to a business owner. And hackers know this. That's why they have had such success with ransomware. Don't let someone take advantage of the effort you have put into your business.

There will be no final victory over malicious actors. But there are steps you can take right now to dramatically reduce your exposures and increase your protection. Don't let your cybersecurity strategy consist of just hopes and prayers. Do something about it.



CYBER FORTRESS CYBER SECURITY CHECKLIST

Print out this page and post it all over your office. Make sure that everyone at your organization is following this checklist. Disregarding it could be the costliest mistake you ever make:

- [ ] Make sure you update all the apps and software that you use so that hackers can't get in through a system that hasn't been patched correctly.
- [ ] Use a password manager to protect against your password being ascertained.
- [ ] Implement two factor authentication for login to protect against unwanted actors gaining access to your secure systems.
- [ ] Use a VPN to access public Internet to protect against hackers.
- [ ] Backup your files using an encrypted, offsite service (Google Drive doesn't count!) to protect against ransomware.
- [ ] Don't open attachments or links from email addresses you do not know to protect against phishing attempts.
- [ ] Install network protection or a firewall to protect against network attacks and breaches.

Remember: security is ultimately about practices and habits, not cutting edge technology and high spending. The most sophisticated security system in the world is useless if you don't know how to turn it on.