GR8 EAGLE
CYBER SECURITY

FREE GUIDE FOR SMALL BUSINESS OWNERS

Cyber Tips for Small Business Owners to Stay Cyber Ready

Practical steps you can take this week to protect your email, payments, devices, and backups — written in plain English for busy owners, not a technical checklist for specialists.

10 actionable tips · No technical jargon required

Gr8 Eagle Cyber
gr8eaglecyber.com · Newark, New Jersey

A free resource from GR8 Eagle LLC

THE FIRST FOUR HABITS

Start with the basics that stop the most common attacks

01

Turn on multi-factor authentication everywhere it is offered

A password alone is not enough. Turn on multi-factor authentication (MFA) for email, banking, payroll, Microsoft 365 or Google Workspace, social media, and any remote-access or VPN login. An authenticator app or hardware key is stronger than a code sent by text message. Start with the accounts that can reset everything else — especially business email.

02

Treat unexpected payment and invoice changes as a red flag

Criminals often impersonate a vendor, employee, or owner and ask you to change a bank account, wire money, or pay a new invoice. If a request arrives by email or text, stop and confirm it using a phone number you already have on file — not a number or link in the message. Make this a written rule for anyone who pays bills or moves money.

03

Keep software and devices up to date automatically

Turn on automatic updates for operating systems, browsers, and apps on company computers and phones. Apply updates on network gear and Wi-Fi routers too, and replace equipment that no longer receives them. Many attacks take advantage of known flaws that a waiting update already fixes.

04

Back up data so you can recover — and test the restore

Use a 3-2-1 approach: three copies of important data, on two different types of storage, with one copy offline or otherwise hard for ransomware to reach. Cloud sync alone is not the same as a backup. A few times a year, practice restoring a file and a full system so you know recovery actually works.

ACCESS, NETWORKS, AND DEVICES

Limit who gets in, and lock down the tools you use every day

05

Use a password manager and give people only the access they need

A password manager lets your team use a unique, strong password for every account without reusing them. Turn off shared “everyone uses the same login” habits where you can. When someone changes roles or leaves, remove their access the same day. Give each person only the systems and privileges their job requires.

06

Lock down business Wi-Fi and be careful with remote work

Use a strong, unique Wi-Fi password and modern encryption (WPA2 or WPA3). Keep a separate guest network for visitors and personal devices. For remote work, avoid signing into banking, payroll, or admin accounts on public Wi-Fi unless you use a trusted VPN. Make sure home-office routers are updated and not left on default passwords.

07

Protect every laptop, phone, and workstation

Require screen locks and device encryption (BitLocker, FileVault, or your phone’s built-in encryption). Keep a reputable endpoint protection tool installed and updated on every computer that handles business data. If a laptop is lost or stolen, you should be able to lock or wipe it remotely. Keep unprotected personal devices out of business email and files.

PEOPLE, PLANS, AND PARTNERS

Prepare your team, your response, and your vendors

08

Make reporting suspicious messages a normal, quick habit

You don't need a long annual class to get value from awareness. Tell your team what a typical phishing or invoice scam looks like, who to tell when something feels off, and that it is always okay to pause and check. A two-minute report can stop an incident that a delayed "I wasn't sure" cannot.

09

Write down a simple incident response plan

One or two pages is enough to start. Name who is in charge, how to reach them, how to isolate an infected computer or lock an email account, where backups live, and which customers, bank, insurer, or IT contacts you would notify. Keep a paper or offline copy. Review it once a year and after any real scare.

10

Protect your email domain and review vendor access

Set up SPF, DKIM, and DMARC on your business domain so it is harder for someone to spoof your email. Review mailbox rules and forwarding from time to time. Give vendors, bookkeepers, and IT partners only the access they need, and turn it off when the work ends. A trusted partner with a weak login can become someone else's way in.

NEXT STEP

Want a clearer picture of your business security posture?

These ten tips are a strong start. Every business is different, though — the right next step depends on the tools you use, who can access them, and how you would recover if something went wrong.

Schedule a free risk assessment or free security scan

Gr8 Eagle Cyber will help you understand where you are solid and where to focus next. There is no obligation. When you are ready, book a call and tell us a little about your business.

Schedule a call at gr8eaglecyber.com/contact

Or email us at **info@gr8eagle.com**
Gr8 Eagle Cyber · GR8 Eagle LLC · Newark, New Jersey

This guide is for general information only. It is not a formal audit, certification, or legal advice, and it is not a substitute for a review of your own environment.