JEFFCOMPUTERS
OVERSEEING CYBERSECURITY

FREE GUIDE

Cybersecurity Guide for Florida Small Business Owners

How to Protect Your Business, Your Data, and Your Customers BeforeIt's Too Late

INSIDE THIS GUIDE:

(941) 759-1120 | jeffcomputers.com

510 Old Venice Rd, Osprey, FL 34229 | Serving Sarasota, Venice, North Port & surrounding areas

info@jeffcomputers.com

What's Inside

All statistics in this guide are drawn from Verizon's Data Breach Investigations Report (DBIR), IBM's Cost of a Data Breach Report, and the FBI's Internet Crime Complaint Center (IC3) — reflecting 2023–2024 data.

CHAPTER 1

Why Small Businesses Are the #1 Target

If you've ever thought, ***'We're too small to be a target,'*** you're not alone. It's one of the most common things we hear from business owners across Sarasota County. And unfortunately, it's also one of the most dangerous assumptions you can make.

The Myth of 'Too Small to Matter'

Hackers don't think about the size of your company — they think about the size of your defenses. Small businesses are attractive targets precisely because they tend to have fewer protections in place, smaller IT budgets, and less employee training around cybersecurity. According to Verizon's Data Breach Investigations Report, 43% of all cyberattacks target small businesses — yet only 14% of small businesses rate their ability to defend against cyber threats as highly effective.

43%	of all cyberattacks target small businesses (Verizon DBIR)
60%	of small businesses close within 6 months of a cyberattack
$200K	average cost of a cyberattack on a small business (IBM)
95%	of data breaches are caused by human error

Why Florida Businesses Face Extra Risk

Florida is the third most targeted state for cybercrime in the US (FBI IC3). There are specific reasons for this:

- High concentration of small businesses in tourism, healthcare, real estate, and professional services, all industries that handle sensitive customer data.
- Large retiree population, making identity theft and elder fraud schemes especially common
- Seasonal businesses with fluctuating staff who may not receive consistent security training
- High volume of remote workers since COVID, expanding attack surfaces without corresponding security upgrades

What Attackers Are Actually After

Mostattacksonsmallbusinessesarefinanciallymotivated and highly automated.

What They Want	Why It's Valuable
Customer payment data	Sold on dark web markets for $5–$50 per card
Employee & payroll records	Used for identity theft and fraudulent tax filings
Business banking credentials	Direct wire transfer fraud — accounts drained same day
Email access	Launched to attack your clients and vendors next
Patient / client records	HIPAA violations can cost $100–$50,000 per record
Ransomware leverage	Lock your files and demand payment to restore access

REAL EXAMPLE

A dental practice in Florida was hit with ransomware. They had no backup. They paid $45,000 to recover their patient records — and then faced a HIPAA investigation on top of it. It could have been prevented with a managed security plan.

CHAPTER 2

The 7 Attack Methods Used Against Florida Businesses

You don't need to be a technical expert to protect your business; you just need to recognize the warning signs. Here are the seven most common attack methods targeting small businesses right now.

1. Phishing Emails

#1 cause of data breaches — 36% of all incidents (Verizon DBIR)

Criminals send emails that look legitimate, your bank, the IRS, Microsoft, a vendor you use and trick you or an employee into clicking a link or entering credentials. Modern phishing emails are remarkably convincing, using real logos and account details obtained from previous breaches.

REAL EXAMPLE

A bookkeeping firm in Sarasota received what appeared to be a QuickBooks security alert. An employee clicked the link, entered their login, and within hours the attackers had accessed three years of client financial data. Recovery cost: over $30,000.

2. Ransomware

Average payment for small businesses: $228,125 in 2023

Malicious software that encrypts all your files documents, customer records, financial data and holds them hostage until you pay a ransom in cryptocurrency. Even if you pay, there's no guarantee you'll get your files back. Ransomware typically enters through phishing emails or outdated software.

3. Business Email Compromise (BEC)

Over $2.9 billion in losses in 2023 (FBI IC3)

A criminal gains access to a business email account (or creates a convincing fake) and uses it to request fraudulent wire transfers or change payment details for invoices. Because the email appears to come from a trusted source, even the CEO, employees often comply without question.

4. Weak or Stolen Passwords

Over 80% of hacking-related breaches involve stolen or weak passwords

Credential stuffing attacks take username/password combinations leaked from other breaches and try them systematically on banking sites, email, and business software. It's automated, and it works far more often than it should, especially when passwords are reused across accounts.

5. Outdated Software & Unpatched Systems

2 months of delayed updates caused the global WannaCry attack

Software companies release security updates specifically to fix vulnerabilities that hackers exploit. When businesses delay or skip updates, they leave known doors wide open. This includes Windows, macOS, routers, accounting software, and anything else connected to your network.

6. Malicious Insiders & Ex-Employees

30% of breaches involve internal actors

Former employees who still have active credentials, or current employees who intentionally or accidentally misuse access, represent significant risk. When an employee leaves, are their accounts immediately deactivated? For most small businesses, the honest answer is no.

7. Unsecured Wi-Fi & Remote Access

Exposed RDP ports are scanned millions of times per day

Home Wi-Fi networks, personal devices, and unsecured Remote Desktop connections (RDP) create opportunities for attackers to access business systems. If your team uses RDP without a VPN, your business is likely being actively scanned by automated bots right now.

BOTTOM LINE

You don't need to be targeted specifically. Most attacks are automated and indiscriminate they scan the internet for vulnerable systems and exploit whatever they find. The businesses that survive are the ones that made themselves slightly harder to attack than the next one.

CHAPTER 3

Your 15-Point Security Self-Audit Checklist

Use this checklist to assess your current security posture. Be honest — the goal isn't a perfect score, it's to find your gaps before someone else does. Print this page and work through it with your team.

SECTION 1 — Passwords & Access Control	
All employee accounts use strong, unique passwords (12+ characters, mixed letters/numbers/symbols)	■
Multi-factor authentication (MFA) is enabled on email, banking, and key business software	■
A password manager is in use (LastPass, 1Password, Bitwarden, or similar)	■
Shared passwords are documented and access is reviewed when staff changes occur	■

SECTION 2 — Software & Patch Management	
Windows / macOS operating systems are set to update automatically	■
All business software (accounting, CRM, email, etc.) is on the current version	■
Antivirus / endpoint protection software is installed on all business devices	■
Router and network equipment firmware has been updated in the last 12 months	■

SECTION 3 — Data Backup & Recovery	
Critical business data is backed up at minimum daily for active files	■
Backups are stored in at least two locations — one of which is offsite or cloud-based	■
Backups have been tested by successfully restoring a file in the last 6 months	■

SECTION 4 — Network & Remote Access	
Wi-Fi uses WPA3 or WPA2 encryption (not WEP or open/no password)	■
A separate guest Wi-Fi network is used for visitors and personal devices	■
Employees working remotely access business systems through a VPN	■
All former employee accounts are deactivated within 24 hours of departure	■

12–15 checked	STRONG — Good security hygiene. Consider a professional audit to verify.
8–11 checked	MODERATE RISK — Several gaps. Prioritise MFA and backups first.
4–7 checked	HIGH RISK — Significant vulnerabilities. Call us for a free consultation.
0–3 checked	CRITICAL — Your business is exposed. Call Jeff Computers today.

CHAPTER 4

Florida Law, HIPAA & PCI — What You Must Have

Depending on your industry, cybersecurity isn't just best practice it's a legal requirement. Failing to meet these requirements can cost more than the attack itself.

Florida Information Protection Act (FIPA)

If your business collects, stores, or processes the personal information of Florida residents, FIPA requires:

- Notify affected individuals within 30 days of discovering a breach
- Notify the Florida Department of Legal Affairs if the breach affects 500+ individuals
- Implement reasonable security measures to protect personal data

Fines can reach up to $500,000. 'Personal information' includes names combined with SSNs, financial account numbers, medical records, and more.

HIPAA (Healthcare & Medical Businesses)

If you handle Protected Health Information (PHI) medical practices, dental offices, therapists, chiropractors, medical billing companies, or any business associate of healthcare providers — HIPAA applies to you.

- Conduct and document a formal risk analysis of where PHI is stored
- Implement access controls — only authorised staff can view patient data
- Encrypt PHI at rest and in transit
- Maintain audit logs of who accessed what data and when
- Maintain a written incident response plan
- Train all employees on HIPAA privacy and security requirements annually

PENALTY RANGE

HIPAA violations range from $100 to $50,000 per violation. In 2023, a small medical practice was fined $100,000 for failing to conduct a risk analysis — the same analysis that would have taken less than a day with professional help.

transaction

PCI-DSS (Any Business That Accepts Credit Cards)

If you accept credit cards in-store, online, or over the phone, PCI-DSS applies, regardless of volume. Key requirements include:

- Use a firewall to protect your payment system network
- Never store full card numbers, CVV codes, or PINs after authorization
- Encrypt card data when transmitted over any network
- Use and regularly update anti-virus software
- Restrict access to cardholder data to staff who need it

Non-compliance can result in fines from your payment processor ($5,000–$100,000/month), loss of ability to accept cards, and liability for fraudulent charges.

CHAPTER 5

What to Do in the First 24 Hours After an Attack

If you discover you've been hacked or suspect a data breach, the first 24 hours are critical. What you do in this window determines how much damage you ultimately suffer. **Print this page and keep it somewhere accessible.**

IMMEDIATE RESPONSE — Hours 0 to 2

1. Do not turn off affected computers immediately. Powering down can destroy forensic evidence. Instead, disconnect from the network (unplug ethernet or disable Wi-Fi) without shutting down.
2. Isolate affected systems from the rest of your network, unplug network cables from switches.
3. Change passwords immediately for all accounts that may be compromised, especially email, banking, and any software containing customer data. Do this from an unaffected device.
4. Enable MFA on any accounts that don't already have it.

DOCUMENT EVERYTHING — Hours 2 to 6

1. Write down or photograph everything you see, error messages, ransomware notes, unusual emails. Timestamps matter.
2. Preserve system event logs, email server logs, and firewall logs if accessible.
3. Note when you first noticed the problem and what normal operations looked like before the incident.

NOTIFY THE RIGHT PEOPLE — Hours 6 to 24

1. Call your IT provider immediately. If you don't have one, call Jeff Computers: (941) 759-1120.
2. Contact your cyber insurance provider if you have a policy, they have incident response teams included.
3. Notify your bank or payment processor if financial accounts or payment systems may be involved.
4. Determine whether FIPA, HIPAA, or PCI-DSS notification requirements are triggered.
5. File a report with the FBI's Internet Crime Complaint Center at www.ic3.gov.

CRITICAL — READ BEFORE ACTING

Do NOT pay a ransom without consulting a cybersecurity professional first. Payment does not guarantee file recovery, may violate OFAC sanctions, and marks you as a paying target for future attacks.

CHAPTER 6

How to Budget for Cybersecurity (Any Size Business)

One of the most common objections we hear: 'We can't afford it.' The truth is, you can't afford not to. But cybersecurity doesn't have to break the bank. Here's a practical framework based on business size and risk level.

The Real Cost of Doing Nothing

The average cost of a data breach for small businesses is $200,000, including forensic investigation, business downtime, customer notification, legal fees, and reputational damage. A comprehensive managed security plan from **Jeff Computers** starts at a few hundred dollars per month — a fraction of the cost of a single incident.

What to Prioritise at Every Budget Level

Budget Level	What to Implement First	Est. Monthly Cost
Minimal $0–$100/mo	MFA on all accounts, password manager, Windows auto-updates, W Defender, Google Drive / On	**~$10 to 50**
Essential $100–$300/mo	All above + business-grade antivirus (Malware, bytes, Bitdefender), backup, basic firewall, phishing	**~$150 to 250**
Managed $300–$800/mo	All above + Managed Detection & Response (MDR), 24/7 monitoring security, regular security	**~$300 to 600**
Full Managed $700+/mo	All above + SOC-as-a-service, SIEM logging, compliance management, (HIPAA/PCI), employee training	**~$500 to 1,200**

Free options like Windows Defender and Google Drive backups are better than nothing. But for businesses that handle sensitive customer data, process payments, or are subject to HIPAA, professional-grade solutions are not optional they are legally required.

BONUS

Get Your Free Security Consultation

You've made it through the guide that means you're taking your business's security seriously, and that's the most important first step. But a guide can only take you so far. Every business has a unique network configuration, different software, different risks, and different compliance obligations. The only way to know exactly where you stand is to have a professional review your specific setup.

Free 15-Minute Security Consultation

No obligation. No sales pressure. Just a real conversation about your current setup and your biggest risks.

(941) 759-1120

info@jeffcomputers.com | jeffcomputers.com/contact-us

Schedule online: jeffcomputers.com/contact-us

What Happens During the Consultation

- We review your current setup, devices, software, and networks you use
- We identify your top 3 risk areas based on your industry and business size
- We explain your legal compliance obligations in plain language
- We recommend a plan that fits your budget whether that's a one-time fix or ongoing managed support

Why Jeff Computers

We're not a national call center. We're your neighbors. Jeff Computers has been serving businesses across Sarasota County for years — from solo accountants in Osprey to dental practices in Venice to restaurants in North Port. When you call us, you talk to someone who knows the area, knows your business type, and will actually show up when something goes wrong.

500+ **FL Businesses Protected**	**24/7** **Monitoring & Support**	**Same Day** **Emergency Response**

Jeff Computers | 510 Old Venice Rd, Osprey, FL 34229 | (941) 759-1120 | jeffcomputers.com

ServingOsprey, Sarasota, Venice, North Port, Nokomis&surrounding communities