

DEVELOPED BY:



WORKSHOP
PRESENTED BY:



MAIN STREET
OAKLAND COUNTY
est. 2000



Cybersecurity Reference Toolkit

Cybersecurity Essentials for Small Business Success

This toolkit, using plain language, is a quick-reference guide for Oakland County small business owners. The guide provides practical steps to reduce cyber risk, respond to incidents, and find trusted, no-cost help – drawing on information from the Federal Trade Commission, Cybersecurity and Infrastructure Security Agency, National Institute of Standards and Technology, National Cybersecurity Alliance, and the State of Michigan. Breach figures come from the Verizon 2026 Data Breach Investigations Report.

**Keep this reference
where it can be
reached quickly if your
business experiences a
cybersecurity incident.**





Contents*

	PAGE
1 Common Cyber Threats	2
2 Phishing & Business Email Compromise	3
3 Passwords & Multi-Factor Authentication	4
4 Building Your Cyber Defenses	5
5 AI Risks & Shadow AI	6
6 Cybersecurity Planning Template	7
7 Incident Management Checklist	8
8 Reporting a Cyber Incident	10
9 Ready Reference: Emergency & Reporting Contacts	11
10 Free Resources	12

Attachment A: Free Cybersecurity Resources

Attachment B: Cybersecurity Planning Template

Attachment C: Incident Management Checklist

Attachment D: Emergency and Reporting Contacts

**These materials were prepared by Compass IT Compliance for Oakland County to provide general guidance and not legal advice.*

Common Cyber Threats

Most attacks on small businesses are not sophisticated. Rather, they rely on a click, a weak password, or an unpatched system. Know the common ones, so your team can spot them.

WHAT TO WATCH FOR:



Phishing and scam messages: fake emails, texts, or calls that trick staff into clicking links, sharing passwords, or wiring money.



Business email compromise (BEC): a criminal impersonates an owner, vendor, or executive to redirect a payment or change banking details.



Ransomware: malicious software that locks your files and demands payment. Often starts with one phishing click.



Stolen or reused passwords: credentials leaked in one breach are tried against your email, banking, and other accounts.



Malware and malicious downloads: infected attachments, fake software updates, or risky websites.



Unpatched software and devices: now the most common way attackers get in, and the exposure is usually the firewall, router, or remote access box rather than a laptop.



Insider mistakes and lost devices: accidental sharing, misconfiguration, or a lost laptop/phone can expose data.

FAST WINS THAT CUT MOST RISK:

- Turn on multi-factor authentication (MFA) for email, banking, and key accounts.
- Patch what faces the internet first, then set everything else to update automatically.
- Back up automatically and restore a real file every three months to prove it works.
- Train staff to pause and verify every payment or banking change by phone on a number you already had.



Phishing & Business Email Compromise

Business Email Compromise (BEC) is the most common route to direct financial loss at this size; though, unpatched internet-facing systems are the most common way attackers first get in.

Artificial Intelligence (AI) now makes these messages look more convincing, including fewer typos, better grammar, and realistic voices.

RED FLAGS IN A MESSAGE:

- Urgency or pressure (“pay now,” “account will close,” “don’t tell anyone”).
- A request to change bank/payment details, buy gift cards, or wire funds.
- Sender address that is slightly off or a display name that does not match the email.
- Unexpected attachments or links. Hover on link to preview the real destination.
- Requests that skip normal process, such as “just this once,” “keep it between us.”

AI-GENERATED PHISHING AND VOICE/VIDEO FAKES:

- Assume grammar and logos can be perfect. Judge the request, not the polish.
- Treat unexpected voice or video from a “boss” or “vendor” as unverified. Deepfakes are cheap to make.

VERIFY BEFORE YOU ACT:

- For any payment or banking change, confirm by phone using a number you already have and not one from the message.
- Use a second person to approve payments over a set dollar amount.
- When in doubt, slow down. Real requests survive a verification call, and no one should ever be criticized for making it.

IF SOMEONE CLICKED OR PAID:

- Disconnect the device from the network, but do not power it off. Change affected passwords from a clean device and sign out all active sessions.
- Call your bank immediately to stop or reverse a transfer and call your insurance carrier before hiring anyone new to help.
- Report it (see the Reporting section), document what happened, and check the mailbox for forwarding rules you did not create.

Passwords & Multi-Factor Authentication

Strong, unique passwords plus Multi-Factor Authentication (MFA) stop most account takeovers. This is the highest-value, lowest-cost step most businesses can take today.

PASSWORDS:

- Use a long passphrase (4+ random words). Length beats complexity.
- Never reuse passwords across accounts, especially email and banking.
- Use a reputable password manager so staff does not have to remember them all.
- Change default passwords on routers, cameras, and other devices.

MULTI-FACTOR AUTHENTICATION (MFA):

- Turn on MFA everywhere it is offered. Start with email, banking, payroll, and remote access. Include the owner's account – there are no exceptions for senior staff or administrators.
- Prefer an authenticator app or security key over text-message codes when possible.
- Never approve an MFA prompt you did not start because that is an indicator that an attacker is trying to get in.

ACCOUNTS & ACCESS:

- Give each employee their own login. Do not use or issue shared accounts.
- Grant only the access each role needs. Remove access the day someone leaves.
- Review who has administrator access at least twice a year.



Building Your Cyber Defenses

A short, repeatable checklist beats a perfect plan you never finish. Work down this list and check the box when it is done.

CORE PROTECTIONS:

- Turn on MFA for email, banking, and all critical accounts.
- Set operating systems, apps, and devices to update automatically – including the firewall, router, and any remote access box.
- Install reputable anti-malware protection and keep it on.
- Back up critical data automatically. Keep one copy offline/offsite. Restore a real file every three months and write down the date.
- Secure your Wi-Fi with a strong password, WPA2/WPA3, and a separate guest network.
- Use a firewall and secure your router (change defaults, keep firmware updated). Set up SPF, DKIM, and DMARC so criminals cannot send email that appears to come from you.
- Encrypt laptops, phones, and any device that stores business data.

PEOPLE AND PROCESS:

- Train staff to spot phishing and to verify payment/banking changes by phone.
- Require dual approval for payments and vendor banking changes.
- Give each person their own account. Remove access promptly when roles change.
- Keep an up-to-date list of your devices, key software, and where data lives.
- Vet vendors and IT providers. Get in writing who has remote access, whether it uses MFA, and what they patch, back up, and monitor.
- Consider cyber liability insurance and know what it requires of you.
- Write down your incident plan and keep contacts handy.

AI Risks & Shadow AI

AI can help small businesses save time. Conversely, it gives attackers new tools. A few simple rules let you use AI safely.

HOW ATTACKERS USE AI:

- More convincing phishing and BEC emails, including clean grammar and tailored to your business.
- Voice and video deepfakes impersonating owners, vendors, or family.
- Faster creation of fraud websites and fake invoices.

“SHADOW AI” – THE QUIET RISK:

- Shadow AI is staff using AI tools without approval, and it is already widespread: 45% of employees are now regular AI users on company devices, up from 15% a year earlier, and 67% reach those tools through personal rather than corporate accounts.
- The danger is that sensitive data (customer info, financials, contracts) gets pasted into tools that may store it or use it to train the model.

TIPS:

- Set a simple rule: No confidential or customer data in public AI tools.
- Pick approved tools and tell staff which ones they can use.
- Treat AI output as a draft. Verify facts, numbers, and code before you rely on them.

USING AI SAFELY AND USEFULLY:

- Good uses include drafting emails, summarizing documents, brainstorming, and first-pass marketing copy.
- Prefer business/paid tiers that do not train on your data and check the privacy settings.
- Keep a human in the loop for anything involving money, contracts, or customers.

Cybersecurity Planning Template

A short plan you actually complete is worth more than a long one that you do not. Update your short plan twice a year. The companion Cybersecurity Planning Template expands each item below into a full plan.

WHAT MATTERS MOST – THE CROWN JEWELS

List the data and systems you cannot operate without – for example customer records, financials, email, point-of-sale, and scheduling:

WHO IS RESPONSIBLE

Security point of contact and who calls the insurance carrier:

IT SUPPORT/PROVIDER

Name and phone number: _____

THE ESSENTIALS AND STATUS

- MFA is on for email, banking, and key accounts.
- Automatic updates are on for devices and software.
- Backups run automatically and a restore has been tested in the last three months.
- Staff have had basic phishing awareness training.
- Payments/banking changes require phone verification + dual approval.

TOP THREE GAPS TO FIX NEXT

1. _____
2. _____
3. _____

NEXT REVIEW DATE

For more information, see **ATTACHMENT B: Cybersecurity Planning Template.**

Keep a human in the loop for anything involving money, contracts, or customers.

Incident Management Checklist

Use this checklist when something goes wrong, such as a suspected breach, ransomware, wire fraud, or an outage.

Work top to bottom. Do not wait to be certain – act on suspicion. The first hour tends to decide both the cost and whether your insurance responds.

STEP ONE – CONTAIN:

- Stay calm. Note the time and what you are seeing.
- Disconnect affected devices from the network (unplug/disable Wi-Fi), do not power off if ransomware, unless advised.
- If money moved, call your bank/payment provider now, by phone, to stop or reverse it.
- Change passwords from a clean device and sign out all active sessions, because a password change alone does not eject someone already logged in. Check for mailbox forwarding rules you did not create.
- Alert your IT support/provider and the owner. Then call your cyber insurance hotline before hiring anyone new, because most policies require their approved responders and hiring your own can reduce or void coverage.

STEP TWO – ASSESS AND DOCUMENT:

- What happened, when did it start, and what/who is affected.
- Is customer or employee personal data involved.
- Preserve evidence: keep logs, emails, and screenshots. Do not wipe systems yet.
- Keep a written log on paper: times, what you saw, who you called, what you changed. If email may be compromised, stop discussing the incident by email and use phone or text.



Incident Management Checklist Continued

STEP THREE – REPORT AND NOTIFY:

- Report to authorities (see Reporting tab): FBI IC3 within 72 hours if money was wired, plus CISA, Michigan MC3, and local law enforcement.
- Do not pay or negotiate on day one. Check nomoreransom.org first, where free decryption tools exist for many ransomware families.
- Determine notification duties (Michigan law may require notifying affected individuals).
- Communicate with staff and, if needed, customers. Keep it factual.

STEP FOUR – RECOVER AND LEARN AFTER INCIDENT:

- Find out how they got in before you restore, or you will restore into the same open door. Then restore from a clean backup and confirm systems are safe before reconnecting.
- Reset credentials broadly and sign out sessions. Keep watching for thirty to sixty days, because attackers and fraudsters both come back.
- Hold a short debrief and include what happened and what to fix.



Reporting A Cyber Incident

Reporting helps you recover, may be required by law, and helps authorities stop the criminals.

Report early - you do not need all the details first.

Life-threatening Emergency	911
FBI - Internet Crime Complaint Center (IC3)	File online at ic3.gov for fraud, BEC, ransomware, and online crime. For a wired payment, file within 72 hours, the window in which funds can realistically be frozen.
CISA (Federal Cyber Agency), 24/7	(888) 282-0870 report@cisa.gov cisa.gov/report
Michigan Cyber Command Center (MC3)	877-MI-CYBER (877-642-9237) mc3@michigan.gov
Report to Local Law Enforcement	File a report with your local police/sheriff. Oakland County Sheriff non-emergency: 248-858-4950 FBI Detroit Field Office: 313-965-2323
Michigan Attorney General - Consumer Protection	877-765-8388 data-breach guidance at michigan.gov/consumerprotection
FTC - Report Fraud and Identity Theft	ReportFraud.ftc.gov IdentityTheft.gov
Your Bank and Payment Processor	Call immediately if money has moved. Number: _____
Your Cyber Insurance Carrier	Call before hiring your own responders. Most policies require their approved panel. Number: _____

Tip: Michigan's Identity Theft Protection Act may require you to notify affected individuals after a data breach. When in doubt, ask your insurer or attorney. Before anyone discusses paying a ransom, check cisa.gov/stopransomware/report-ransomware for free decryption tools.

For more information, see ATTACHMENT C: Incident Management Checklist

Ready Reference

Fill in your local details and post them where staff can see the information.
Update names and numbers when they change.

For more information, see ATTACHMENT D: Emergency and Reporting Contacts

EMERGENCY AND LOCAL	
Emergency Police, Fire, and Medica	911
Local Police/Sheriff for Non-Emergency	Oakland County Sheriff: 248-858-4950
Utility/Power	DTE 800-477-4747 Consumers Energy 800-477-5050
Building/Facilities Contact	

YOUR BUSINESS RESPONSE TEAM	
Owner / Decision-Maker	_____
Security Point of Contact	_____
IT Support / Managed Service Provider	_____
Bank/Payment Processor:	_____
Fraud Line	_____
Cyber Insurance Carrier	Policy Number: DIFS Complaints: 877-999-6442
Attorney	_____

REPORTING	
FBI IC3 (online crime)	ic3.gov
CISA (24/7)	(888) 282-0870 report@cisa.gov
Michigan MC3	877-MI-CYBER mc3@michigan.gov
MI Attorney General - Consumer Protection	877-765-8388
FTC	ReportFraud.ftc.gov IdentityTheft.gov

Free Resources

Trusted, no-cost help from U.S. government agencies and nonprofits you can bookmark, plus:

- NIST's Small Business Cybersecurity Corner nist.gov/itl/smallbusinesscyber
- Global Cyber Alliance Toolkit gcatoolkit.org/smallbusiness
- Cyber Readiness Institute cyberreadinessinstitute.org

For more information, see **ATTACHMENT A: Free Cybersecurity Resources**

FEDERAL:

- **FTC - Cybersecurity for Small Business:** Plain-language basics, videos, and free guides. ftc.gov/business-guidance/small-businesses/cybersecurity
- **National Cybersecurity Alliance - CyberSecure My Business:** Free resources, training, and templates for owners. staysafeonline.org/programs/cybersecure-my-business
- **CISA - Cyber for Small Business:** Federal cyber agency. Free tools, alerts, and reporting. cisa.gov
- **SBA - Strengthen Your Cybersecurity:** Guidance and no-cost resources for small businesses. sba.gov
- **FCC - Cybersecurity for Small Businesses:** Tips and a customizable cyber planning tool. fcc.gov

STATE OF MICHIGAN

- **Michigan Cyber Command Center (MC3):** State cyber incident help and reporting. michigan.gov/msp | 877-MI-CYBER | mc3@michigan.gov
- **MI Attorney General - Consumer Protection:** Data-breach and identity-theft guidance. michigan.gov/consumerprotection
- **Michigan SBDC:** Free consulting and training, plus the free Small Business, Big Threat cyber self-assessment. michigansbdc.org - 833-522-0025
- **Small Business Association of Michigan (SBAM):** "Be Protected & Secure" cybersecurity guidance for MI businesses. sbam.org

IN AN EMERGENCY, DIAL 911. Report a cyber incident to CISA 24/7: (888) 282-0870
FBI IC3: ic3.gov | Michigan MC3: 877-MI-CYBER



Attachment A | Free Cybersecurity Resources

A reference for small and mid-sized businesses

Every resource in this guide is free for the described tier, and nearly all come from a government agency, a nonprofit, or an open community project. Two commercial-free tiers are included and clearly labeled. Nothing here requires a purchase.

You are not expected to use all of it. Pick the three items under Start Here, then use the 90-day plan on the last page to sequence the rest. Free resources fail for one reason: nobody owns them. Assign a name to each item you adopt.

Start here, in this order

1. Michigan SBDC, Small Business, Big Threat. Take the free self-assessment first, so you know where you stand. Michigan advisors will follow up at no cost. michigansbdc.org
2. Global Cyber Alliance, Cybersecurity Toolkit for Small Business. Six concrete steps with the tools built in. Work through it in order. gcatoolkit.org/smallbusiness
3. FTC, Cybersecurity for Small Business. Short videos and printable fact sheets to share with staff. ftc.gov

FEDERAL RESOURCES

FTC - Cybersecurity for Small Business

Federal Trade Commission

Short videos and plain-language guides on the risks small firms actually face.

ftc.gov/business-guidance/small-businesses/cybersecurity

FTC - Protecting Small Businesses

Federal Trade Commission

Guides, sample policies, and free training on scams, data security, and vendor risk.

ftc.gov/business-guidance/small-businesses

FTC - Fact sheet set (PDF)

Printable handouts

One page per topic. Print these and hand them to staff.

ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_sb_factsheets_all.pdf

SBA - Strengthen your cybersecurity

Small Business Administration

Step-by-step guidance and a directory of no-cost resources.

sba.gov

FCC - Cybersecurity for Small Businesses

Federal Communications Commission

Practical tips plus a customizable cyber planning tool that produces a written plan.

fcc.gov

CISA - Secure Our World and free services

Cybersecurity & Infrastructure Security Agency

Four basic habits explained for non-technical staff, plus a catalog of no-cost tools and services.

cisa.gov/secure-our-world

cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

NIST - Small Business Cybersecurity Corner

National Institute of Standards and Technology

Vendor-neutral guides, planning worksheets, and the Cybersecurity Framework 2.0 small business quick-start guide.

nist.gov/itl/smallbusinesscyber

MICHIGAN AND REGIONAL RESOURCES

Michigan SBDC - Small Business, Big Threat

State partner | free assessment

No-cost training, a free self-assessment, and follow-up help from real advisors.

michigansbdc.org

Small Business Association of Michigan

- Be Protected and Secure

Trade association

Cybersecurity guidance tailored for Michigan businesses.

sbam.org

Michigan Cyber Command Center (MC3)

Michigan State Police

State assistance during a cyber incident.

Call 877-MI-CYBER (877-642-9237) or email mc3@michigan.gov.

michigan.gov/msp (MC3)

Michigan Attorney General

- Consumer Protection

State agency

Data breach notification and identity theft guidance. Consumer line 877-765-8388.

michigan.gov/consumerprotection

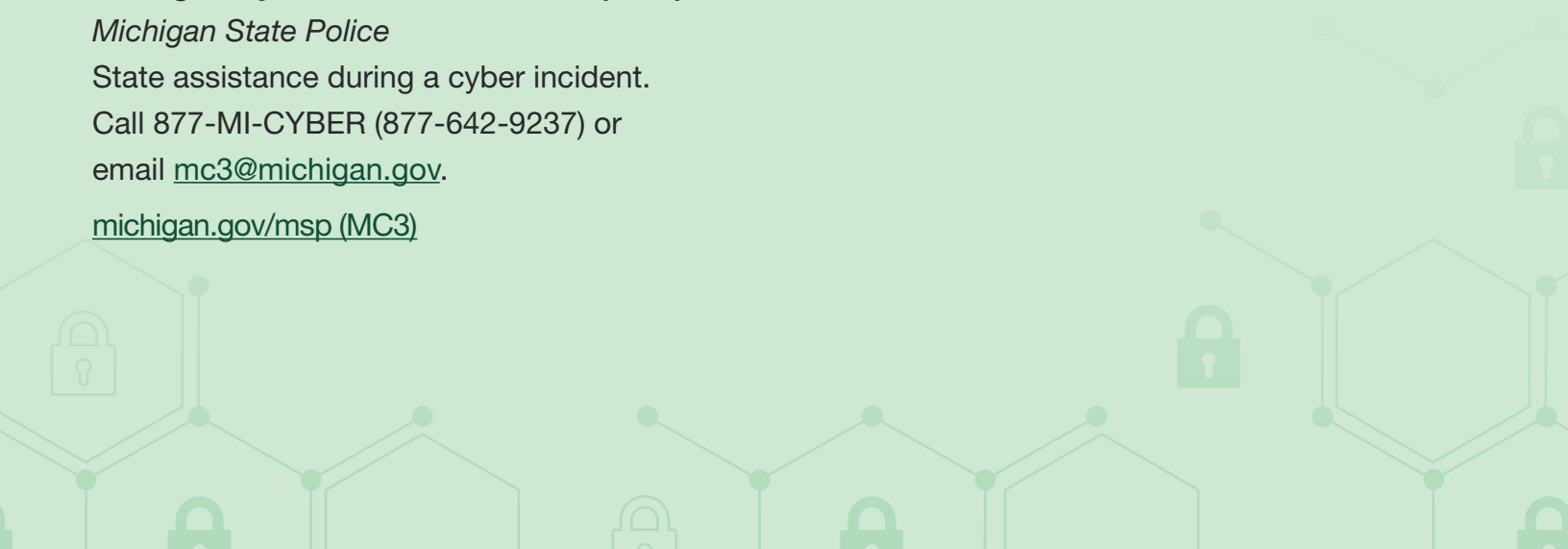
Michigan DIFS - Insurance help

State agency

Questions or complaints about insurance carriers, including cyber policies.

Call 877-999-6442.

michigan.gov/difs



NONPROFIT PROGRAMS BUILT FOR SMALL BUSINESSES

These are the resources most small businesses have never heard of and benefit from most. They are independent of any vendor, and several are the source material that federal guidance points back to.

Global Cyber Alliance - Cybersecurity Toolkit for Small Business

Nonprofit

Six guided steps with free tools built in, aligned to the CIS Controls. The best single starting point if you have no IT staff.

gcatoolkit.org/smallbusiness

Cyber Readiness Institute - Cyber Readiness Program

Nonprofit | free program

Self-paced program that walks one designated “cyber leader” through four core policies, with ready-made templates and staff training.

cyberreadinessinstitute.org

National Cybersecurity Alliance - CyberSecure My Business

Nonprofit

Educational modules and templates covering basic cybersecurity practices.

staysafeonline.org

Center for Internet Security - CIS Controls and Benchmarks

Nonprofit

The prioritized control list most auditors and insurers recognize. Start with Implementation Group 1. Benchmarks give free hardening settings for Windows, macOS, and cloud services.

cisecurity.org/controls

cisecurity.org/cis-benchmarks

Institute for Security and Technology - Blueprint for Ransomware Defense

Nonprofit | Ransomware Task Force

Forty plain-language safeguards written for small firms, now mapped to NIST CSF 2.0. Estimated to address roughly 70 percent of common ransomware attack paths.

securityandtechnology.org

OWASP Foundation

Nonprofit

Free application security guidance if you build, host, or commission custom software or a customer-facing web app.

owasp.org

Nonprofit Cyber

Coalition

A coalition of nonprofit cybersecurity organizations. Useful for finding vetted free resources without wading through vendor marketing.

nonprofitcyber.org

SECURITY AWARENESS AND STAFF TRAINING

Most incidents at small firms start with a person, not a firewall. A monthly five-minute habit beats an annual training video nobody remembers.

SANS - OUCH! newsletter

Free, monthly

A one-page awareness newsletter in plain English, translated into 25+ languages. Forward it to staff each month; it is the cheapest awareness program available.

sans.org/newsletters/ouch

SANS - Free workforce resources

Free downloads

Posters, tip sheets, and ready-to-run Cybersecurity Awareness Month campaign kits.

sans.org/for-organizations/workforce/resources

Cyber Readiness Institute - Employee Training Toolkit

Free

Short training on the four issues that cause most small-business incidents: passwords, updates, phishing, and removable media.

cyberreadinessinstitute.org

National Cybersecurity Alliance - awareness materials

Free

Shareable graphics, videos, and campaign guides you can put in a newsletter or break room.

staysafeonline.org

CISA - Secure Our World toolkits

Free

Posters, videos, and tip sheets covering MFA, passwords, updates, and phishing.

cisa.gov/secure-our-world

Wizer - free awareness training

Commercial vendor, free tier

Short video-based training with a genuinely free tier that suits very small teams. Listed for completeness; the free tier is limited.

wizer-training.com

FRAMEWORKS, CHECKLISTS, AND SELF-ASSESSMENTS

Use one of these as your target state so “are we secure?” becomes a question with an answer. Insurers, lenders, and larger customers increasingly ask which framework you follow.

CIS Controls Implementation Group 1

Nonprofit

The recognized definition of “essential cyber hygiene” for organizations with limited IT expertise. Use it as your target state.

cisecurity.org/controls

NIST CSF 2.0 Small Business Quick-Start Guide

Federal

A short, readable guide to organizing security work into six functions. Good for board or lender conversations.

nist.gov/itl/smallbusinesscyber

UK NCSC - Small Business Guide and Cyber Action Toolkit

UK government | free

Answer a few questions and get a personalized, prioritized action plan with progress tracking. The clearest plain-English security writing available anywhere, and it is not UK-specific.

ncsc.gov.uk/collection/small-business-guide

ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations

THREAT INTELLIGENCE AND EARLY WARNING

You do not need a threat intelligence team. You need to know when something on your own network is exposed, and which vulnerabilities are being exploited right now. Both are available free.

Shadowserver Foundation

- free daily network reports

Nonprofit | highest value on this page

After a one-time verification that you own your IP space, Shadowserver emails you a daily report of exposed services, unpatched vulnerabilities, and infections it sees on your network. Free, no contract, used by 10,000+ organizations.

shadowserver.org/what-we-do/network-reporting/get-reports/

CISA - Known Exploited Vulnerabilities catalog and alerts

Federal | free

The authoritative “patch this now” list. Ask your IT provider to confirm nothing on it is unpatched in your environment. Free email alerts available.

cisa.gov/known-exploited-vulnerabilities-catalog

Have I Been Pwned

Free tier

Check whether staff email addresses appear in known breaches. The free tier includes monitoring for domains with up to 10 breached addresses, plus the free Pwned Passwords check.

haveibeenpwned.com

SANS Internet Storm Center

Free

Daily analyst commentary on what attackers are doing right now. Skim the diary weekly.

isc.sans.edu

abuse.ch - URLhaus and ThreatFox

Nonprofit | free feeds

Community-run blocklists and indicator feeds your IT provider or firewall can consume at no cost.

abuse.ch/

MITRE ATT&CK

Nonprofit | free

A catalog of real attacker techniques. Useful for asking a vendor or MSP precise questions about what they actually detect.

attack.mitre.org

National Council of ISACs

Directory

Find the information-sharing center for your industry. Sector ISACs often have low-cost or free tiers for small members.

nationalisacs.org/

Verizon Data Breach Investigations Report

Free annual report

The best free evidence base on how breaches actually happen, including a dedicated small-business section.

verizon.com/business/resources/reports/dbir/

AI SECURITY AND GOVERNANCE

Two separate problems live under the word “AI.” The first is governing the AI tools your staff already use, whether or not you approved them. The second is defending against attackers who use AI, most visibly through voice and video impersonation in payment fraud. The resources below cover both.

OWASP GenAI Security Project

Nonprofit | the reference for AI risk

The Top 10 for LLM Applications, the new Top 10 for Agentic Applications, and a practical guide to preparing for and responding to deepfake events.

genai.owasp.org

NIST - AI Risk Management Framework

Federal | voluntary

A free framework and companion playbook for governing how your organization adopts AI. Use it to structure an AI policy rather than inventing one.

nist.gov/itl/ai-risk-management-framework

SANS - Critical AI Security Guidelines

Free framework

Control-oriented guidance for deploying AI tools safely, aligned to NIST AI RMF, ISO 42001, and OWASP.

sans.org/mlp/critical-ai-security-guidelines

Cloud Security Alliance - AI resources

Nonprofit | registration required

Free AI Controls Matrix and AI governance guidance for organizations buying or deploying AI services.

cloudsecurityalliance.org

CISA and NSA

- AI Data Security best practices

Federal

Joint guidance on protecting the data that AI systems are trained on and operate against.

cisa.gov

Three AI actions worth doing this quarter

- Inventory what is already in use. Ask staff which AI tools they use for work. The answer is almost never “none,” and free consumer accounts often have no data protections at all.
- Publish a one-page acceptable-use policy. State plainly which categories of information may never be pasted into a public AI tool: customer records, financial data, health information, credentials, and anything under contract or regulatory protection.
- Require callback verification for money movement. Voice and video impersonation is cheap and convincing now. Any change to payment details or any urgent transfer request gets verified by calling a known number, never a number supplied in the request. Put this in writing and tell staff they will never be penalized for making the call.

FREE TOOLS AND SERVICES

Practical controls you can enable yourself or delegate to your IT provider. The first two, protective DNS and DMARC, deliver more risk reduction per hour spent than anything else on this page.

Quad9 and Cloudflare 1.1.1.1 for Families

Free protective DNS

Change one setting on your router or devices and known malicious domains stop resolving. One of the highest-return free controls available.

quad9.net/ | one.one.one.one/family/

Global Cyber Alliance - DMARC setup guide

Free walkthrough

Stops criminals from sending email that appears to come from your domain. This is the control that reduces invoice and payroll fraud.

dmarc.globalcyberalliance.org

Internet.nl

Free test

Tests your website and email against modern security standards, including SPF, DKIM, DMARC, and TLS, and explains each result.

internet.nl/

Qualys SSL Labs server test

Free test

Grades your website's encryption configuration and tells you what to fix.

ssllabs.com/sslttest

VirusTotal and urlscan.io

Free lookups

Check a suspicious file, link, or website before anyone clicks it. Good tools to teach your office manager.

virustotal.com/ | urlscan.io/

CIS-CAT Lite

Nonprofit | free tool

Scores a Windows or macOS machine against the CIS Benchmarks so you can see what is misconfigured.

learn.cisecurity.org/cis-cat-lite

Bitwarden and KeePassXC

Free tier / open source

Password managers a small business can actually deploy at no cost. Shared passwords in a spreadsheet are a common finding in every assessment.

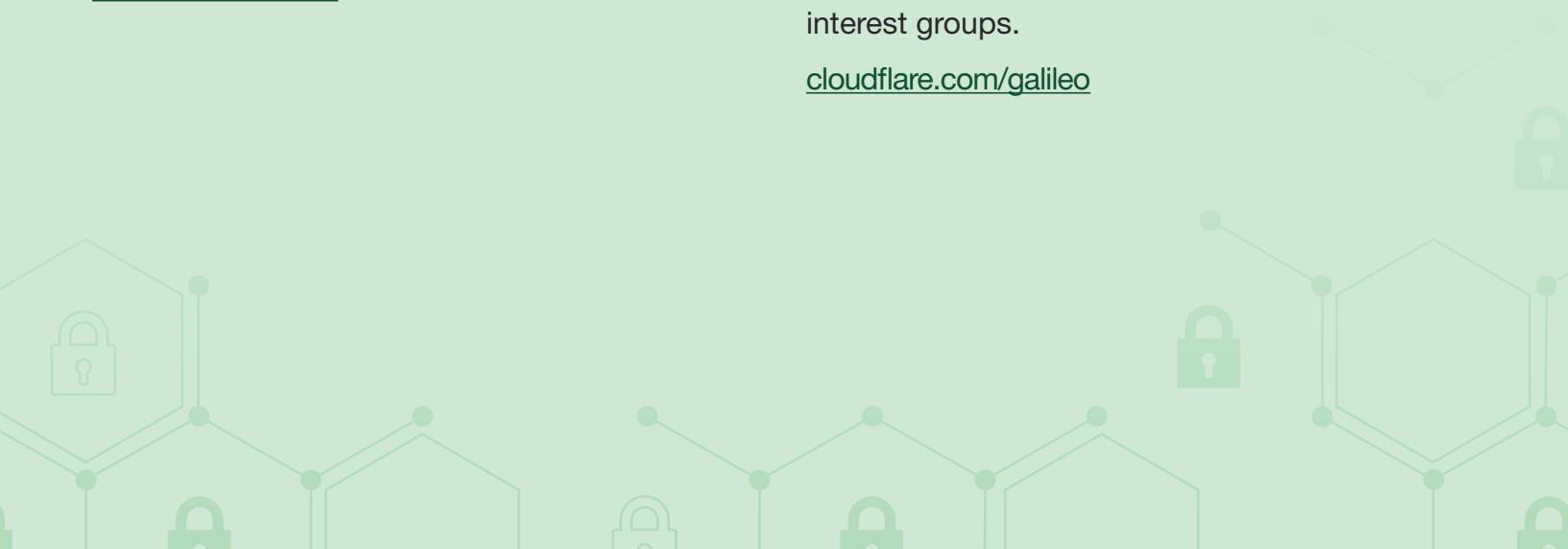
bitwarden.com/ | keepassxc.org/

Cloudflare Project Galileo

Free for qualifying organizations

Free DDoS and web application protection for nonprofits, civil society, and at-risk public-interest groups.

cloudflare.com/galileo



RANSOMWARE AND INCIDENT RESPONSE

The time to read this section is before you need it. A one-page plan and one practice run put you ahead of most organizations your size.

No More Ransom

Europol and partners | free

Free decryption tools covering roughly 200 ransomware families, plus Crypto Sheriff to identify which strain hit you. Check here before anyone discusses paying.

nomoreransom.org

StopRansomware.gov

Federal

Consolidated federal guidance, including the joint ransomware guide and a response checklist.

stopransomware.gov

ID Ransomware

Community project | free

Upload a ransom note or sample file to identify the strain and whether a free decryptor exists.

id-ransomware.malwarehunterteam.com

CISA - Tabletop Exercise Packages

Federal | free

Ready-made scenario packages with facilitator notes and discussion questions.

cisa.gov

REPORTING AN INCIDENT

Save these where staff can reach them without logging into a company system, because during an incident they may not be able to. Report even when you expect no recovery. Reporting is how patterns are seen, and funds are occasionally frozen.

FBI Internet Crime Complaint Center (IC3)

Report first, and fast

Report cybercrime, ransomware, and wire fraud. For fraudulent wire transfers, report within 72 hours to give the FBI Recovery Asset Team the best chance of freezing funds.

ic3.gov

Michigan Cyber Command Center (MC3)

877-MI-CYBER | 877-642-9237

State incident assistance for Michigan organizations. Email mc3@michigan.gov.

michigan.gov/msp

CISA | 888-282-0870

Report incidents, especially if they affect services other organizations depend on.

cisa.gov/report

FTC

Fraud and identity theft

Report business fraud and get recovery plans for affected individuals.

reportfraud.ftc.gov | identitytheft.gov

Michigan Attorney General

877-765-8388

Breach notification obligations and identity theft guidance for affected Michigan residents.

michigan.gov/consumerprotection

Michigan DIFS | 877-999-6442

Questions or complaints involving insurance carriers, including cyber claims.

michigan.gov/difs

STAYING INFORMED

Two or three of these is plenty. The goal is to hear about something that affects you before a customer does.

- **SANS NewsBites and @RISK:** free semiweekly and weekly summaries written for practitioners.
sans.org/newsletters
- **CISA alerts:** free email notifications of active threats and urgent patches.
cisa.gov
- **Krebs on Security:** independent investigative reporting that frequently covers small-business fraud.
krebsonsecurity.com
- **BleepingComputer:** fast, readable coverage of ransomware and breaches.
bleepingcomputer.com
- **Dark Reading:** twenty years of industry news and analysis, more technical than the general tech press.
darkreading.com
- **FTC Business Blog:** plain-language alerts on scams targeting businesses.
ftc.gov
- **StateScoop:** state and local government IT and cyber news, including funding and policy changes that affect available help.
statescoop.com
- **MMRMA:** Michigan public entity risk pool; cyber coverage for members, plus RAP and CAP grants that can help fund security projects.
mmrma.org
- **NACo, Cybersecurity for Counties:** county cybersecurity resources and MS-ISAC enrollment. However, note that the page's no-cost claim is outdated.
naco.org/page/cybersecurity-counties
- **FEMA NIMS:** the incident command structure governments use to coordinate any incident, including cyber; free training, and required for federal preparedness grant eligibility.
fema.gov/emergency-managers/nims

NOTES ON USING THIS LIST

- Assign an owner to every item you adopt. Free resources fail from lack of ownership, not lack of quality.
- Several resources require registration or a verification step. Read what you are agreeing to share, particularly where you are asked to confirm ownership of your IP address ranges or domains.
- MS-ISAC is still widely recommended as a source of free threat intelligence. That advice is out of date. Federal funding ended on September 30, 2025. Membership is now fee-based, and it remains limited to state, local, tribal, and territorial government entities. It is not an option for private small businesses. Shadowserver and the CISA KEV catalog cover most of the same practical ground at no cost.
- Be skeptical of a vendor's free security scan or dark web report offered as a lead-generation tool. The findings are usually real but presented to maximize alarm. Nothing on this list requires a purchase to be useful.
- Links were verified in July 2026. Government reorganizations and changes in program funding can break links. If one fails, search for the organization's name plus "small business."

YOUR FIRST 90 DAYS

Every item below uses a free resource from this guide. Nothing here requires new spending, and none of it requires a specialist.

First 30 days

- Turn on multifactor authentication for email, banking, remote access, and every administrator account.
- Take the free Michigan SBDC Small Business, Big Threat self-assessment and keep the result.
- Work through Steps 1 to 3 of the Global Cyber Alliance toolkit: know your devices, patch them, fix passwords.
- Check your domain in Have I Been Pwned and force resets on any exposed accounts.
- Post the reporting numbers on this sheet where staff can find them without logging in.

Days 31 to 60

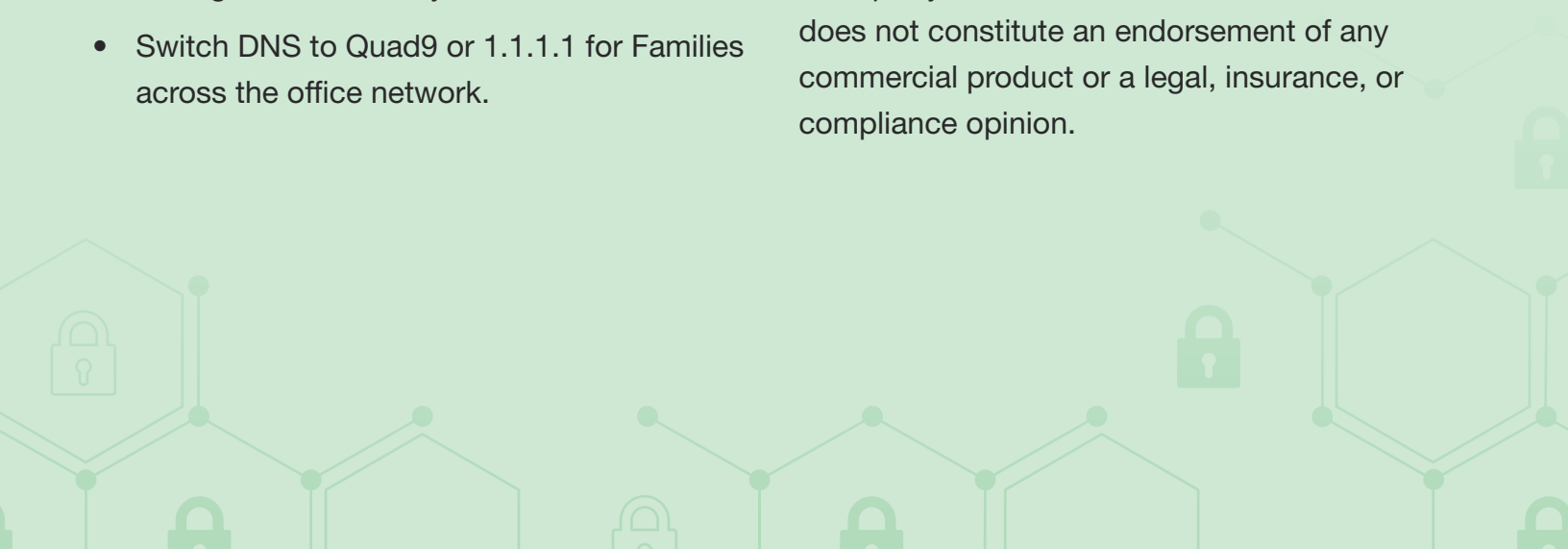
- Subscribe to Shadowserver's free daily reports for your own IP space and act on what comes back.
- Name one cyber leader and enroll them in the Cyber Readiness Institute program; adopt the four core policies.
- Configure SPF, DKIM, and DMARC using the GCA guide, then verify with [Internet.nl](https://internet.nl).
- Switch DNS to Quad9 or 1.1.1.1 for Families across the office network.

- Start forwarding the OUCH! newsletter to all staff monthly.
- Test a restore from backup. An untested backup is not a backup.

Days 61 to 90

- Compare your current state against CIS Controls Implementation Group 1 or the Blueprint for Ransomware Defense and write down the gaps.
- Draft a one-page incident response plan, then run the Exercise in a Box ransomware scenario against it.
- Inventory the AI tools staff are already using and publish a one-page acceptable-use policy.
- Review your cyber insurance application answers against reality and confirm which controls the policy requires.
- Get your IT provider's security responsibilities in writing, including patching, backup, and monitoring.

Prepared as part of Cybersecurity Essentials for Small Business Success. This guide lists third-party resources for convenience and does not constitute an endorsement of any commercial product or a legal, insurance, or compliance opinion.





Attachment B | Cybersecurity Planning Template

A working plan you can adopt today

Most planning templates hand you blank pages and hope for the best. This one is already filled in. It contains a plan that fits the vast majority of small businesses, written in plain English, with sensible choices made for you.

Your job is to read it once, cross out anything that does not apply to you, and fill in fewer than a dozen blanks, all of which sit in three short spots. This will result in a written security plan, which is more than most businesses your size can say they have. No technical background is needed anywhere in this document.

How to use this

- Read it start to finish once. Do not stop to look anything up.
- Cross out what does not apply to your business. Deleting is faster than writing.
- Fill in the blanks in Part 2, Part 8, and the sign-off at the end. Everything else is already written for you.
- Save it where more than one person can find it and keep a printed copy. During a real problem, you may not be able to open a file.
- Part 4 is written to be shared with everyone who works at your organization. You can lift it out and hand it to the staff as is. The other parts are for whoever runs the business or leads on security.

The whole plan, in six sentences

- Almost nothing that hits a business is targeted. Attackers scan the internet for exposed systems and reused passwords, then work through whoever answers.
- Two controls close most of the doors: two-step login on email and remote access, and prompt patching of anything facing the internet.
- A backup you have actually restored from is what decides whether ransomware is a bad week or the end of the business.
- Your largest single loss will probably not be ransomware. It will be someone quietly changing bank details inside an email thread you already trust.
- Roughly half your risk now sits with your vendors and your IT provider, so their controls are your controls.
- If something happens, call your insurer before you call anyone else, and report wire fraud to ic3.gov within 72 hours.

PART 1. WHY THIS PLAN LOOKS THE WAY IT DOES

Among the small-business breaches examined in the Verizon 2026 Data Breach Investigations Report, the attacker came from outside the business in every single case, and the motive was money in every single case. Criminals scan for open doors and work through whoever answers.

Exploiting an unpatched weakness is now the most common way in, at 31 percent of all breaches, up from 20 percent the year before. It is not usually a laptop that is exposed. It is the equipment connecting the office to the internet, and across all organizations, only about a quarter of the weaknesses on the government's actively-exploited list were fully

fixed during 2025. Stolen passwords and convincing emails account for most of the rest. Ransomware was involved in nearly half of all breaches, and when the size of the victim was known, roughly 96 percent were small and mid-sized businesses.

One number explains the shape of Part 4. A person was involved in 45 percent of small-business breaches, so staff awareness matters but is one control among several rather than a plan on its own. The rules are ordered to close the doors above, with the most useful first, and none of them require technical skill or new spending.

PART 2. WHO IS RESPONSIBLE

Plans fail because nobody owns them, not because they are wrong. Write a name in every row. None of these roles requires technical skill.

ROLE	WHAT THIS MEANS
Security lead	Makes sure the items in this plan actually happen. Usually the owner, office manager, or operations lead. This is a coordinating job, not a technical one.
IT support	Your internal person or outside provider. Write the number you would call at 7 pm on a Friday, not the general office line.
Approves payments and payment changes	Should be someone other than the person who enters payments, so two sets of eyes are involved.
Calls the insurance company	Usually the owner. See Part 8 for why this call comes first.
Owens backups and tests them	Can be the same as IT support but name a person rather than a company.

If the same name appears in every row, that is completely normal at a small-sized organization. Write it down anyway. The point is that the responsibility has been stated out loud instead of assumed.

PART 3. WHAT YOU CANNOT OPERATE WITHOUT

This is pre-filled with what nearly every small business depends on. Cross out anything you do not use.

- Email and calendar
- Customer records, contact lists, and quotes
- Accounting, invoicing, and payroll
- Card payments or point-of-sale system
- Orders, scheduling, or job management
- Files, documents, and photos
- Phones and voicemail
- The website and anything customers book or buy through it

Anything else specific to your entity: _____

Whatever you did not cross out is exactly what your backups, your insurance, and your IT provider need to cover. If you are not certain what all three do, that is your first question to ask this week.

PART 4. SECURITY RULES

These rules are the plan. They are written so you can adopt them exactly as they stand and hand them to staff. Each one includes the reason, because rules people understand are the rules people follow. They are ordered by how much risk they remove, so the first four matter most.

- **Turn on two-step login, starting with email, and** *[add other applications or systems as applicable]*: Email is the master key to your business, because password resets for banking, payroll, and every cloud service arrive there. Turn it on for email first, then banking, then remote access,

then every administrator account. An authenticator app or a physical key is safer than a texted code, because criminals now talk people into reading the code out. Include the owner's account. No exceptions for senior staff or system administrators, which is where this usually breaks down.

Free help: gcatoolkit.org/smallbusiness
cisa.gov/secure-our-world

- **Patch what faces the internet, and know what that is:** Updates should

install automatically on every computer, phone, and app. The bigger exposure is usually not a laptop. It is the box that connects your office to the internet, the firewall, router, or remote access gateway, and it is the one nobody thinks of as a computer. Ask your IT provider for written confirmation each month that nothing on the government's actively-exploited list is unpatched in your environment.

Free help: CISA KEV catalog
 Shadowserver free daily reports

- **Keep backups you have actually restored from:** A backup counts only if it runs automatically, keeps at least one copy offline or otherwise out of reach so ransomware cannot encrypt it too, covers your cloud data as well as your servers, and has been used to restore a real file within the last three months. Microsoft 365 and Google Workspace are not backups on their own. They faithfully copy whatever happens, including deletions or attacks. Write the date of each successful test in Part 7.

Free help: Blueprint for Ransomware Defense | nomoreransom.org

- **Verify every payment change by voice, on a number you already had:** This is the single rule most likely to save you real money, and it rarely looks like an attack. A criminal reads an email thread they have gained access to, then sends a believable note changing where a payment goes. Any change to payment details, and any urgent transfer request, is confirmed by calling a

number from your own records, never a number supplied in the message. Treat a familiar voice as proof of nothing, because voice and video can now be imitated cheaply. Two people approve any payment over [\$XX.xx]. No one in this business will ever be criticized for delaying a payment to make the call, and saying that out loud is what makes the rule work.

Free help: OWASP deepfake response guide
ftc.gov/small-businesses

- **Give every person their own login, and remove it the day they leave:** Shared logins mean you cannot tell who did what, and access cannot be cleanly shut off when someone goes. Work through the same short list every time: email, remote access, every online service, the password manager, banking and payroll, building keys or door codes, and the person's registered two-step login device. This applies to contractors and bookkeepers, too, who are most often forgotten.

Free help: Cyber Readiness Institute policy templates

- **Stop criminals sending email that looks like it came from you:** Three settings on your domain, known as SPF, DKIM, and DMARC, prevent this. It is a one-time job for whoever manages your domain, it costs nothing, and it directly blunts the payment fraud described in the rule above. It also stops your customers receiving fake invoices in your name. Have it done, then verify it independently rather than taking anyone's word for it.

Free help: GCA DMARC setup guide | internet.nl

- **Build a five-minute monthly habit instead** of an annual video: Forward one short awareness piece to all staff each month, and talk through a real example at a staff meeting twice a year. Most training covers only email, but phone calls and text messages are now just as common a way in, so include those. Consistency beats production value.

Free help: SANS OUCH! newsletter
CRI Employee Training Toolkit
- **Use a password manager, and keep passwords out of spreadsheets, notebooks, and sticky notes:**
A password manager is an app that remembers long, different passwords for every account so people do not have to. Reused passwords are one of the most common ways businesses get broken into, because a password stolen from somewhere else gets tried on your accounts.
- **Keep a short list of approved software and AI tools, and ask before adding new ones:** The plain rule for AI tools: never paste customer records, financial details, health information, passwords, or anything covered by a contract into a public AI tool. Staff are already using these tools, so give them an approved option rather than a ban they will quietly ignore. Part 5 explains why this now matters more than it did.
- **Anyone can report something that looks wrong, immediately and without blame:** Most of the damage comes from the delay, not from the original click. Say plainly and often that reporting a mistake quickly is considered good judgment. If people are afraid, you will find out last.
- **Guests use a separate Wi-Fi network from your business systems:** Most business routers can do this in a few minutes. It keeps a visitor's infected laptop away from the computers that run your business.

PART 5. THREE THINGS THAT CHANGED RECENTLY

AI is already inside your business, whether or not you approved it. Across monitored organizations, 45 percent of employees are now regular users of AI tools on company devices, up from 15 percent a year earlier, and 67 percent are reaching those tools through personal rather than corporate accounts. Unauthorized AI use is now the third most common non-malicious insider action seen in data-loss monitoring. You do not need to

ban anything, and a ban would not hold. State which categories of information may never go into a public AI tool, then list the approved tools, so people have a legitimate option.

Attackers use AI too, but the practical effect is narrower than the headlines. What has genuinely changed is volume and polish. Fluent, well-researched phishing in any language, and voice or video impersonation

convincing enough that recognizing a familiar voice proves nothing. That makes the payment verification rule more important, not a new problem. The defense is procedural, not technical.

Your vendors are now a large share of your risk. A third party was involved in 55 percent of small-business breaches. The remote

management software your IT provider uses to help you is also one of the most useful tools an attacker can find. Ask three questions and get the answers in writing: who has remote access to our systems, is that access protected by two-step login, and what exactly are you responsible for patching, backing up, and monitoring? A provider who cannot answer plainly is telling you something.

PART 6. WHAT GOOD ENOUGH LOOKS LIKE AT YOUR SIZE

Security advice is usually written for organizations with a security team. Here is a realistic target by headcount. Each tier assumes that the one above it is already done.

1 to 20 people

No IT staff

- Cloud-based email and files, so you inherit a large vendor's security instead of running your own.
- Two-step login on email, banking, and remote access. A password manager for everyone.
- A managed backup service you have restored from.
- A payment verification rule in writing, plus a short monthly note to staff.
- No security tooling beyond that, which is the correct answer at this size.

20 to 100 people

One generalist IT person or an outside provider

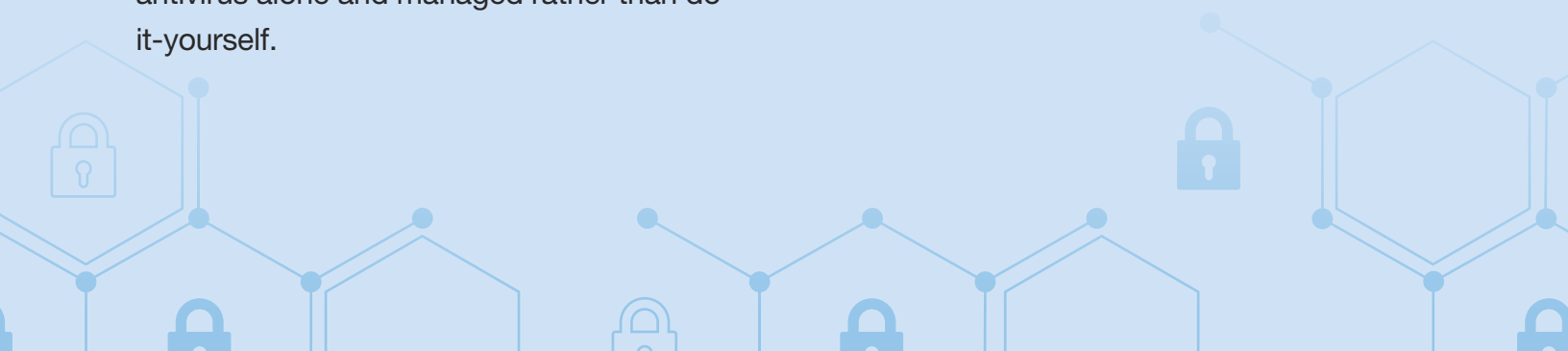
- Managed threat monitoring rather than antivirus alone and managed rather than do-it-yourself.

- A written patching commitment from your provider, confirmed monthly.
- A documented joiner and leaver process that someone actually follows.
- Cyber insurance where your application answers match what you truly have in place.

100 to 250+ people

Approaching real complexity

- A named person accountable for security can be a part-time or contracted role rather than a hire.
- A written gap assessment against a recognized baseline, revisited annually.
- A security review of any vendor holding your data or holding remote access.
- Quarterly restore tests, and activity logs kept long enough to answer questions afterward.



PART 7. WHAT KEEPS THIS PLAN ALIVE

A plan written once and filed away stops being true within a year. This rhythm is what turns it into something real, and none of it takes long.

Every month

- Share one short security tip or story with staff. Five minutes at a team meeting is enough.
- Confirm backups actually ran, rather than assuming they did.
- Ask IT support to confirm that urgent security updates have been applied.

Every three months

- Restore one real file from backup and write down the date.
- Review who has access to email, banking, and payroll, and remove anyone who no longer needs it.

Twice a year

- Reread this plan and update the names and phone numbers.
- Check that bank, insurance, and IT contacts are still correct.

Once a year

- Spend thirty minutes talking through Part 8 out loud with the team, as a what-if conversation. Free ready-made scenarios are listed at the end of this document.
- Review your insurance coverage and what it requires you to have in place.
- Ask your IT provider for a written summary of what they are responsible for, so there is no gap between what you assumed the other was covering.

PART 8. IF SOMETHING GOES WRONG

Read this now rather than during the event. The first hour tends to determine both the cost and whether your insurance responds. The companion Incident Management Checklist covers the same ground in more detail, including what to do in the first ten minutes. Print that one and keep it where staff can reach it without logging in.

1. Isolate, do not power down. Disconnect the affected machine from the network by unplugging it or turning off Wi-Fi. Shutting it down destroys evidence stored in memory that responders use to determine how far the problem spread.
2. Call your cyber insurer's hotline before anyone else. Most policies require you to use their approved responders and legal counsel. Hiring your own first can reduce or void coverage, and this is the single most expensive mistake small businesses make in the first hour. Calling your existing IT provider is fine and should happen straight away.
3. Call your IT provider, and call your bank if money moved. Ask the bank directly for a recall or freeze by phone. Do not send an email about it.
4. Report it. File with the FBI at ic3.gov, and for a fraudulent wire transfer, do so within 72 hours, which is the window during which the FBI Recovery Asset Team can realistically

freeze funds. Then contact the Michigan Cyber Command Center at 877-MI-CYBER for state assistance.

5. Do not pay or negotiate on day one, and check nomoreransom.org first. More than 160 free decryption tools there cover roughly 200 ransomware families and variants, and 69 percent of victims in the Verizon data did not pay.
6. Keep a written log on paper or a personal device: times, what you saw, who you called, what you changed. Do not keep it in the affected systems.
7. Ask early whether personal information was involved, because that triggers notification obligations. The Michigan Attorney General's office can advise at 877-765-8388.

NUMBERS TO HAVE BEFORE YOU NEED THEM

Cyber Insurance Hotline And Policy Number	_____
IT Support, After Hours	_____
Bank Fraud Line	_____
Report Cybercrime, FBI	ic3.gov
Michigan Cyber Command Center	877-MI-CYBER (877-642-9237)
Michigan Attorney General, Consumer Line	877-765-8388
Free Ransomware Recovery Tools	Nomoreransom.org

PART 9. YOUR FIRST 90 DAYS

Everything below uses a free resource. None of them requires new spending or a vendor call.

First 30 days

- Turn on two-step login for email, banking, and remote access, including the owner's account.
- Restore one file from backup. If you cannot, you have just found your top priority.
- Implement a written payment verification rule and give it to whoever pays bills.
- Print the Incident Management Checklist and put it somewhere staff can reach without logging in.

Days 31 to 60

- Take the free Michigan Small Business Development Center (SBDC) self-assessment and keep the result michigansbdc.org/
- Set up the password manager and get everyone using it.
- Ask your IT provider to configure the settings that stop criminals sending email that looks like it came from you.
- Start sharing one short security tip with staff each month.

Days 61 to 90

- Work through the free Global Cyber Alliance small business toolkit (gcatoolkit.org/smallbusiness/), in order.
- Spend thirty minutes walking through Part 8 as a group.
- Get your IT provider's responsibilities in writing.
- Review insurance coverage against what this plan says you actually do.

Where to get free help

Each rule in Part 4 identifies the free resource that applies to it. These three are the general starting points, and the companion resource guide lists many more.

- Michigan SBDC, a free self-assessment and no-cost advice from real advisors. michigansbdc.org
- Global Cyber Alliance, a six-step toolkit built for businesses with no IT staff. gcatoolkit.org/smallbusiness
- Free practice scenarios for the yearly what-if conversation in Part 7.

Adoption and review

Adopted on: _____ by: _____

Next review date: _____ (pick a date six months out and put it in the calendar now)

Our single biggest gap right now: _____

Prepared by Compass IT Compliance for Oakland County. Statistics from the Verizon 2026 Data Breach Investigations Report. General guidance, not legal advice





Attachment C | Incident Management Checklist

A 10-minute read now, so you can act in the first ten minutes later

This document works two ways. Read it once now, while nothing is wrong. That is what the ten minutes are for. Then print the action card below and put it somewhere your staff can access it without logging in. During a real incident, nobody is going to read five pages, and the systems holding your nice digital copy may be the ones that are down.

It covers cyber problems such as a fraudulent payment, ransomware, a stolen laptop, or a compromised email account, and operational disruptions such as a power cut or an internet outage. The order of operations is much the same for both.

The first ten minutes - print this part

Act on suspicion. You do not need to be certain that something is wrong to start.

- Note the time and what you are seeing. Use paper.
- Make people safe first if there is any physical risk. Everything else can wait.
- Disconnect affected computers from the network. Unplug the cable or switch off Wi-Fi. Do not power them off.
- If money moved, phone the bank's fraud line immediately and ask them to recall it.
- Call your IT support and the owner or manager.
- Call your insurance carrier's hotline before you hire anyone new to help.
- Stop using email to discuss this if email might be affected. Switch to phone or text.

Two habits that decide how this goes

Act on suspicion, not certainty:

The most expensive incidents are almost never the ones nobody noticed. They are the ones somebody noticed on Tuesday, felt unsure about, and raised on Friday. Nobody in your business should ever be criticized for reporting something that turns out to be nothing. Say that out loud, more than once, before anything happens.

Get off the channel that might be

compromised: If there is any chance an attacker is inside your email, then every message your team sends about the incident is being read by them. Move the conversation to phone calls or text messages until you know otherwise. This one habit catches people out constantly, because email is the natural place to coordinate.

STEP 1. CONTAIN AND STABILIZE

Safety comes before equipment, and equipment comes before data. If anyone is at physical risk, deal with that and nothing else.

For a cyber problem, disconnect the affected machine from the network rather than shutting it down. Unplug the network cable or turn off Wi-Fi. Powering the machine off wipes information held in its memory, which is often how a specialist works out what happened and whether anything else is affected. Leave it running but isolated unless your IT provider tells you otherwise.

If money has moved, this is the most time-sensitive thing on the page. Call your bank or payment processor on their fraud line, by phone, and ask them to recall or freeze the transfer. Then report it to the FBI at ic3.gov within 72 hours. That window is where the

FBI's recovery team has a realistic chance of stopping the funds. After it closes, the odds fall sharply.

If an account has been broken into, reset the password from a device you trust, not from the affected one. Then do the step most people miss - sign out all active sessions, sometimes labeled "sign out everywhere." Changing a password on its own does not eject someone who is already logged in. While you are there, check the mailbox for forwarding rules or filters you did not create. Attackers routinely add a hidden rule that quietly copies or deletes messages, so you do not see the replies.

STEP 2. CALL YOUR INSURER BEFORE YOU HIRE ANYONE

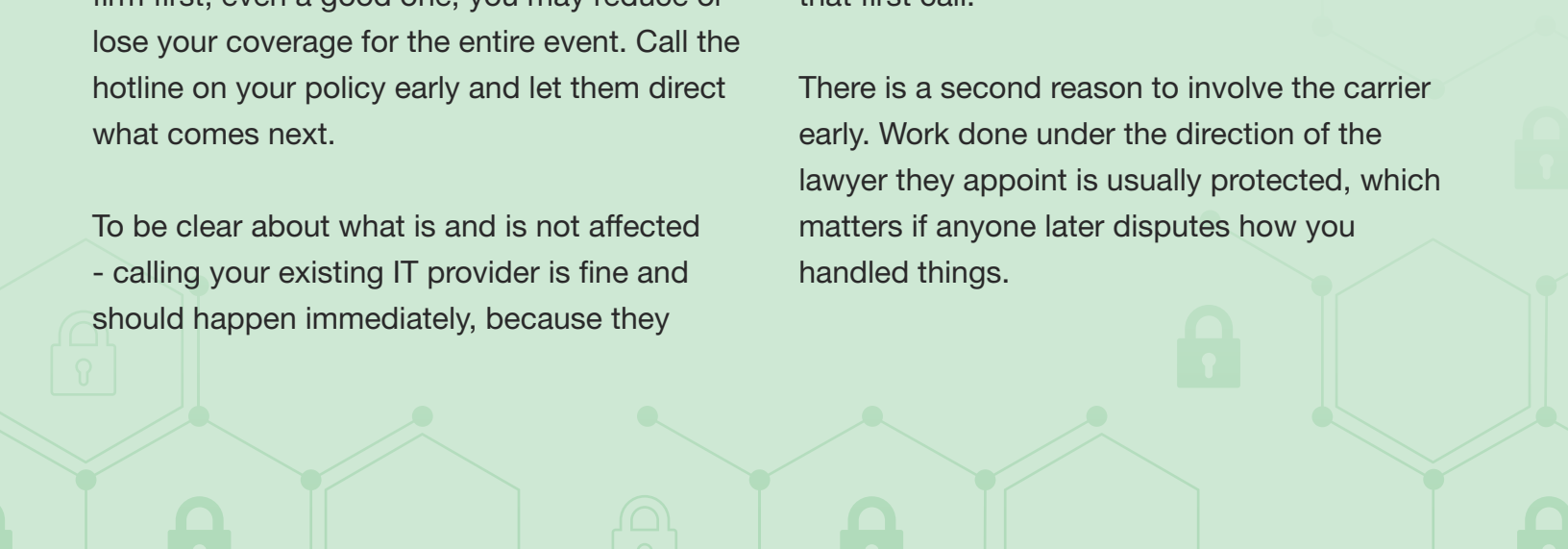
This step is separated out because getting it wrong is expensive and the mistake is easy to make in good faith.

Most cyber insurance policies require you to use responders and lawyers from their approved list. If you engage your own forensics firm first, even a good one, you may reduce or lose your coverage for the entire event. Call the hotline on your policy early and let them direct what comes next.

To be clear about what is and is not affected - calling your existing IT provider is fine and should happen immediately, because they

already work for you. The restriction is about bringing in new outside help. If you are unsure whether something counts, ask the carrier on that first call.

There is a second reason to involve the carrier early. Work done under the direction of the lawyer they appoint is usually protected, which matters if anyone later disputes how you handled things.



STEP 3. ASSESS AND WRITE IT DOWN

Keep a running log on paper or on a phone, not on the systems that may be affected. Record the time, what you saw, who you called, and what you changed. This log becomes the backbone of your insurance claim, any report you file, and any conversation with a customer or regulator.

Answer four questions as best you can, and write “unknown” where you do not know rather than guessing:

- What happened, and when did it start?
The start is usually earlier than the moment you noticed.
- Which systems, accounts, or people are affected?
- Could customer or employee personal information be involved? This is the question that determines whether you have legal duties later.
- Is it still happening, or has it stopped?

Preserve the evidence. Do not wipe, reinstall, or “clean up” anything yet, however tempting. Keep the emails, take photographs of screens, and save any ransom note exactly as it appeared. Ask your IT provider today to preserve and export the activity logs from your email and key systems, because many services only keep those for a limited period and they will quietly disappear while you are busy with everything else.

Stick to observed facts in anything you write. Speculation about cause or blame written down in the first hours has a way of resurfacing later, and it is usually wrong.

STEP 4. REPORT IT

Reporting is not publicity. These are confidential channels, not announcements, and filing a report does not put your business in the news.

- FBI Internet Crime Complaint Center, for any cybercrime or fraud. Within 72 hours if money was wired. ic3.gov
- CISA, the federal cyber agency, on (888) 282-0870, particularly if the disruption affects services other people rely on.
- Michigan Cyber Command Center, on 877-MI-CYBER (877-642-9237), for state assistance.
- Local law enforcement, for theft, a physical break-in, or any threat to safety. Use 911 if anyone is in danger.

Report even when you expect nothing to come of it. Recovery does sometimes happen, and your report is part of how the pattern gets spotted for the next business.

STEP 5. NOTIFY PEOPLE IN THE RIGHT ORDER

Order matters here, because saying the wrong thing early is hard to undo.

- Your insurer first, as above.
- Then your staff, with what they actually need, including what not to click, what not to pay, and who to route questions to. Tell whoever handles payments to hold anything unusual until further notice.
- Then customers and partners, once you have facts rather than fears. Say what you know, what you are doing, and when you will update them next. Do not promise what you cannot confirm, and do not say no data was affected until somebody competent has actually checked.
- Then anyone you are legally or contractually required to tell. Michigan law can require notifying individuals after a breach of personal information, and your customer contracts may set their own deadlines, sometimes shorter than the law's. Your insurer's appointed lawyer will guide this.

Pick one person to be the single voice for the business. Mixed messages from several well-meaning people cause more reputational damage than the incident usually does.

STEP 6. RECOVER WITHOUT REINFECTION YOURSELF

The most common way businesses end up with a second incident is restoring everything before understanding how the first one started. If you put the systems back exactly as they were, the door that was used is still open.

- Work out the entry point first, or have your provider confirm it. Then close it before you reconnect anything.
- Bring systems back in a deliberate order and confirm each is clean before the next reconnects.
- Restore from a backup taken before the incident began, and have it checked before you trust it.
- Keep watching for thirty to sixty days. Attackers and fraudsters both come back, often through a different door and sometimes using information they took the first time.
- Reset passwords across the business, not just the obvious accounts, and sign out all sessions.

Meanwhile, keep the business running by whatever means work. A mobile hotspot for internet, card payments by phone, a paper order pad. Deciding in advance which three services must come back first, and in what order, turns a chaotic day into a manageable one.

STEP 7. TWO WEEKS LATER, HOLD A SHORT REVIEW (LESSONS LEARNED)

Book 30-60 minutes within 2 weeks of the incident being resolved, while people still remember it clearly. Four questions should be addressed:

- What actually happened?
- What slowed us down?
- What went well?
- What two things will we change?

Two changes that get done beat ten that get written up. Then do the unglamorous part. Update the phone numbers in this document, tell your IT provider what you learned, restore a test file to prove your backups still work, and check whether your insurance covered what you assumed it would. As your organization continues to mature its Cyber Incident Response, you can conduct a more robust lessons-learned review.

Practice this once before you need it

Reading a plan and using one are different skills. Spend thirty minutes a year walking a scenario through out loud with your team - no technology required, just the question "what would we actually do?"

Free, ready-made scenarios with facilitator notes are available from CISA's tabletop exercise packages. Businesses that have rehearsed once behave completely differently in the first hour cisa.gov/cisa-tabletop-exercise-packages.

WHAT NOT TO DO

- Do not power off a machine you suspect has ransomware, unless your IT provider says to.
- Do not hire your own forensics or legal help before speaking to your insurer.
- Do not keep discussing the incident by email if email might be compromised.
- Do not wipe, rebuild, or reinstall anything until the evidence is preserved.
- Do not pay a ransom on the first day. Check nomoreransom.org, which offers free decryption tools for many ransomware families, and take advice before anyone discusses payment.
- Do not tell customers that no data was affected until somebody has actually verified it.
- Do not leave one person to handle it alone through the night. Tired people make expensive decisions.

IF IT IS AN OUTAGE RATHER THAN AN ATTACK

Power cuts, internet failures, burst pipes, and weather follow the same shape. Make people safe, protect equipment and data, tell staff and customers what is happening, switch to your fallback, and review afterward. Two things are worth deciding in advance rather than on the day: which services must come back first, and what your alternative is for each one. A mobile hotspot, a second internet line, a manual payment process, and a printed customer contact list will cover most of what a small business needs.

NUMBERS TO HAVE READY

Fill in the blanks, print this page, and keep a copy somewhere reachable without a computer. Add it to phones as contacts too.

Emergency: police, fire, medical	911
Your insurance carrier and policy number	_____
Your IT support, 24-hour number	_____
Your bank or payment processor, fraud line	_____
Local police, non-emergency	_____
FBI Internet Crime Complaint Center	ic3.gov
CISA, federal, 24/7	(888) 282-0870
Michigan Cyber Command Center	877-MI-CYBER (877-642-9237)
Michigan Attorney General, consumer line	877-765-8388
Free ransomware decryption tools	nomoreransom.org

Prepared by Compass IT Compliance for Oakland County. General guidance, not legal advice.



Attachment D | Emergency and Reporting Contacts

Print and post where staff can see it without logging in. Fill in the shaded blanks. Check the numbers once a year.

Most planning templates hand you blank pages and hope for the best. This one is already filled in. It contains a plan that fits the vast majority of small businesses, written in plain English, with sensible choices made for you.

Your job is to read it once, cross out anything that does not apply to you, and fill in fewer than a dozen blanks, all of which sit in three short spots. This will result in a written security plan, which is more than most businesses your size can say they have. No technical background is needed anywhere in this document.

If something has just gone wrong, do these first

Act on suspicion. You do not need to be certain. Nobody here is ever criticized for reporting something that turns out to be nothing.

- ☐ Note the time and what you are seeing on paper. Make people safe first if there is any physical risk.
- ☐ Unplug the affected computer from the network or turn off its Wi-Fi. Do not power it off.
- ☐ If money moved, phone the bank fraud line now and ask for a recall.
- ☐ Call IT support and the owner. Then call the insurer before hiring anyone new to help.
- ☐ If email may be affected, stop discussing it by email. Use phone or text.

Before you change any payment details

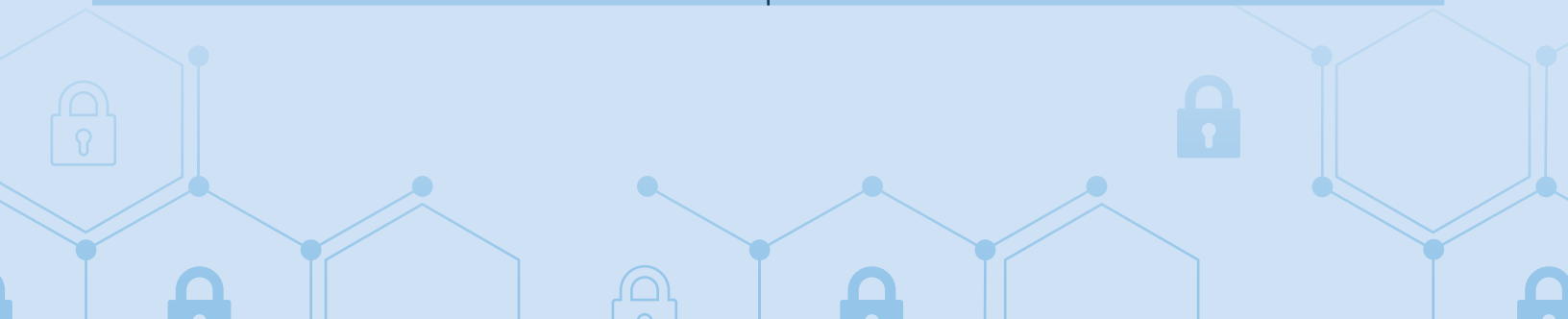
Call the requester back on a number you already had, never a number from the message, and get a second approver. A familiar voice proves nothing. Slowing a payment down to make that call is always the right decision.

EMERGENCY AND RESPONDERS

Life-threatening emergency	911 police, fire, medical
Oakland County Sheriff, non-emergency	248-858-4950 confirm this covers your location
Your local city police, non-emergency	_____ <i>[department and phone]</i>
Oakland County Emergency Management	248-858-5300 oakeoc@oakgov.com free OakAlert notifications at Oakgov.com
Gas leak	Leave the building, then call 911. DTE 800-947-5000. Consumers Energy 800-477-5050.
Power outage or downed line	DTE 800-477-4747. Consumers Energy 800-477-5050. Verify which is your provider.

CYBERCRIME AND FRAUD REPORTING

FBI Internet Crime Complaint Center	ic3.gov report wire fraud within 72 hours, which is the window to freeze funds
FBI Detroit Field Office	313-965-2323 tips.fbi.gov , 24/7
CISA, federal cyber agency, 24/7	888-282-0870 report@cisa.gov
Michigan Cyber Command Center	877-MI-CYBER (877-642-9237) mc3@michigan.gov
Michigan Attorney General	877-765-8388 consumer protection, breach notification duties
FTC, fraud and identity theft	ReportFraud.ftc.gov IdentityTheft.gov
Hit by ransomware	nomoreransom.org free decryption tools. Check here before anyone discusses paying.



YOUR BUSINESS: FILL THESE IN

Insurance claims or incident hotline	Call this before hiring your own responders
Cyber insurance carrier and policy number	<i>[carrier, policy number]</i>
Agent or broker	<i>[name and phone]</i>
Bank or payment processor, fraud line	<i>[24-hour phone]</i>
Owner or decision-maker	<i>[name and mobile]</i>
Security point of contact	<i>[name and mobile]</i>
IT support or managed provider	<i>[company and 24-hour phone]</i>
Attorney	<i>[name and phone]</i>
Michigan DIFS, insurance complaints	877-999-6442 <i>questions or complaints about a carrier</i>

*Prepared by Compass IT Compliance for Oakland County. Numbers verified July 2026.
General guidance, not legal advice*

