GUERILLA SECURITY

What Everyone Needs to Know

2026

A plain-language guide to protecting yourself, your organization, and the information entrusted to you — for employees, customers, board members, and executives.

Andrew T. Robinson
RESCOR LLC
521 Lincoln Road, West Enfield, ME 04493
+1 863 SECURE1 (+1 863 732-8731)
www.rescor.net

Contents

Guerilla Security: What Everyone Needs to Know

Why This Matters to You

Every organization depends on technology. The systems you use every day — email, file sharing, banking portals, patient records, cloud applications — contain information that someone, somewhere, wants to steal, lock up, or exploit.

You don't need to be a security expert to protect yourself and your organization. But you do need to understand three things:

1. **Attacks will happen.** No system is perfectly secure. The question is not whether someone will try — it's whether you're prepared when they do.
2. **You are a target.** Attackers don't just go after servers and firewalls. They go after people — through deceptive emails, phone calls, text messages, and websites. People are often the easiest way in.
3. **You are also the best defense.** Technology catches many threats automatically. But the threats designed to fool technology are designed to fool *you*. Your ability to recognize, pause, and report something suspicious is a layer of protection that no software can replace.

This guide covers what you need to know — in plain language, without jargon.

For Leaders: Why This Is Your Responsibility

If you serve on a board of directors, in executive leadership, or in any management role, security is part of your fiduciary responsibility — whether or not it appears in your job description.

The legal landscape has changed. Directors and officers face personal liability in some jurisdictions for failure to exercise adequate oversight of cybersecurity risk. The SEC requires publicly traded companies to disclose material cybersecurity incidents within four business days. HIPAA, GLBA, and state privacy laws impose penalties that can dwarf the cost of the breach itself. The question regulators and courts ask is not "was there a breach?" but "did leadership take reasonable steps to prevent it?"

You don't need to understand the technology. You need to understand five things:

1. **What is our risk?** Not in colors (red, yellow, green) — in numbers you can compare and trend. If your security team can't express risk quantitatively, they can't manage it.
2. **Are we investing proportionately?** Security spending should be driven by measured risk, not by fear, compliance checklists, or vendor pitches. A control that costs more than the risk it mitigates is waste.

3. **Can we detect and respond — not just prevent?** Organizations that invest only in prevention discover breaches months later. Organizations with detection and response capabilities contain them in days. Ask for mean time to detect and mean time to respond as board metrics.
4. **What happens when — not if — we're breached?** Is there an incident response plan? Has it been tested this year? Does it include regulatory notification timelines? Who makes the call to notify regulators, customers, and the press?
5. **Are our people engaged or just compliant?** A workforce that completes annual security training and clicks through the quiz is compliant. A workforce that actually recognizes phishing, reports suspicious activity, and follows procedures is secure. These are not the same thing.

The rest of this guide applies to you too. Board members get phishing emails. Executives get targeted by social engineering. Leadership credentials are among the most valuable targets an attacker can compromise — because they carry the most access and the most authority.

The Threats You'll Actually Face

Phishing: The #1 Attack on People

Phishing is a deceptive message — usually email, but also text messages, phone calls, or social media — designed to trick you into doing something: clicking a link, opening a file, entering your password, or transferring money.

Modern phishing is sophisticated. The messages:

- Come from addresses that look legitimate (sometimes from real accounts that have been compromised)
- Reference real projects, real people, and real events at your organization
- Are written in perfect grammar with no obvious errors
- Create urgency: "Your account will be locked," "Invoice overdue," "CEO needs this immediately"

What to do:

- **Pause before clicking.** If a message asks you to do something — especially something urgent or unusual — take ten seconds to think before acting.
- **Verify through a different channel.** If you get an email from your boss asking you to buy gift cards, call your boss. Don't reply to the email — the attacker controls the email. Pick up the phone or walk to their office.
- **Look at the actual link.** Hover over links (don't click) to see where they really go. A link that says "mybank.com" but points to "myb4nk-secure.com" is not your bank.
- **Report it.** If something looks suspicious, report it. You won't get in trouble for reporting something that turns out to be legitimate. You might prevent a breach by reporting something that isn't.

Phone and Voice Attacks

Not all attacks come by email. "Vishing" (voice phishing) uses phone calls to impersonate IT support, your bank, a vendor, or even a colleague. With modern AI, an attacker can clone someone's voice from a few seconds of public audio.

What to do:

- Be suspicious of unsolicited calls asking for passwords, account numbers, or remote access to your computer.
- If someone calls claiming to be from IT or your bank, hang up and call back using a number you know is correct — not the number they gave you.

- Never give your password to anyone over the phone. Legitimate IT support does not need your password.

Ransomware: What It Is and Why You Matter

Ransomware is software that locks your files (or your entire computer) and demands payment to unlock them. Modern ransomware also steals your data before locking it, threatening to publish it if you don't pay.

Ransomware usually gets in through phishing (you click something you shouldn't) or through a security weakness in a system connected to the Internet. Once inside, it can spread to every computer on the network.

Why you matter: Most ransomware attacks start with a single person clicking a single link or opening a single attachment. Your caution is the first line of defense.

What to do:

- Don't open attachments you weren't expecting, even if they appear to come from someone you know.
- If your computer starts behaving strangely — files won't open, your screen shows a ransom message, programs are running that you didn't start — **disconnect from the network immediately** (unplug the network cable or turn off Wi-Fi) and call IT or your security contact.
- Speed matters. The faster a ransomware infection is reported, the less it can spread.

Passwords: What Actually Works

You've probably been told to create passwords with uppercase letters, lowercase letters, numbers, and special characters, and to change them every 90 days. That advice is outdated and actually makes things worse.

Here's what the research shows:

Length Beats Complexity

A long passphrase like **"purple mountain highway sunset"** is both harder to crack and easier to remember than **"P@ssw0rd!"**. Length is what makes passwords strong — not special characters.

- Use passphrases of four or more random words, or sentences that are meaningful to you but hard to guess.
- Aim for at least 16 characters. Longer is better.
- Don't use personal information (birthdays, pet names, addresses) that someone could find online.

Don't Reuse Passwords

If you use the same password for your work email and your personal shopping account, and the shopping site gets breached, the attacker now has your work email password too. Attackers test stolen passwords against every major service automatically.

- Use a different password for every account that matters.
- Use a password manager to keep track of them. You only need to remember one strong master password.

Don't Rotate Unless Compromised

Frequent password changes cause people to choose weaker passwords (Password1, Password2, Password3) or write them on sticky notes. Change your password when there's a reason to — if you suspect it's been compromised, or if you're notified of a breach at a service you use. Otherwise, a strong password that you keep is better than a weak password that you change.

Multi-Factor Authentication (MFA)

MFA adds a second verification step beyond your password — typically a code from an app on your phone, a push notification, or a physical key. Even if an attacker steals your password, they can't get in without the second factor.

Use MFA on any account that is accessible remotely or that touches sensitive information — email, banking, cloud services, VPN, patient records, financial systems. MFA is the single most effective protection against stolen credentials used from another location. Your organization's security team determines where MFA is required based on the risk; if you have the option to enable it and it isn't already required, enable it.

Watch out for:

- **MFA fatigue attacks.** If you receive repeated MFA approval prompts that you didn't initiate, **do not approve them.** Someone is trying to get into your account. Deny the prompts and report it immediately.
- **Fake login pages.** An attacker sends you to a page that looks like your real login. You enter your password and MFA code. The attacker captures both in real time and uses them before the code expires. This is why verifying URLs matters.

Your Phone Is Your Most Critical Asset

Your phone has become the keys to your digital life. It receives text codes, push notifications, and calls. It runs your authenticator app. It may store your passkeys. If you lose your phone — or it breaks, gets stolen, or gets replaced — and it's your only MFA method, you could be locked out of dozens of accounts simultaneously. A lost phone without a screen lock is even worse: whoever finds it has your authenticator, your push notifications, and your SMS codes.

Always use a PIN, fingerprint, or face lock on your phone. Always.

If you're upgrading to a new phone, export your authenticator data *before* you wipe the old one. Most authenticator apps (Google Authenticator, Microsoft Authenticator) support transfer or cloud backup — but only if you set it up in advance. Biometric enrollments (fingerprint, face) don't transfer — you'll need to re-register them on the new device, which requires authenticating through the mechanisms that depend on the biometrics you can no longer use. Plan ahead.

Report a lost or stolen phone immediately to your IT department or security contact. Treat it as a security incident — because it is one.

Protect Your MFA — Before You Need To

The best protection against phone loss is having backup MFA methods already in place.

Set up backup methods now, before something goes wrong:

- **Register more than one phone number** for accounts that support SMS or voice backup — your own number plus a trusted family member's. The family member doesn't need access to your account — they just need to be able to receive a one-time code and read it to you.

- **Save your recovery codes.** When you set up MFA, most services generate one-time recovery codes. Print them and store them somewhere safe — not on the same phone as your authenticator app. These codes are your last-resort way back in.
- **Register a backup email** for services that support email-based recovery.
- **Know your organization's recovery process.** If you lose all your MFA methods, how do you get back in? Who do you contact? Find out now — not during the emergency.

If you are ever locked out and cannot recover your account through self-service, your organization should have a way for you to reach a human who can verify your identity and restore access. If that process doesn't exist, tell your security team — because the alternative is permanent lockout, which is not acceptable for accounts you need to do your job or manage your health and finances.

Protecting Sensitive Information

Know What's Sensitive

Not all information requires the same protection. But some categories require extra care:

- **Personal information** — Social Security numbers, financial account numbers, health records, dates of birth
- **Credentials** — Passwords, PINs, security questions, MFA recovery codes
- **Business confidential** — Financial reports, customer lists, trade secrets, strategic plans
- **Patient/client data** — Protected health information (PHI), customer financial data

Handle It Carefully

- Don't send sensitive information by email unless it's encrypted. Email is not secure by default.
- Don't paste sensitive data into AI tools (ChatGPT, Copilot, etc.) unless your organization has specifically approved it. The data may be retained by the provider.
- Don't store sensitive information on personal devices, USB drives, or personal cloud storage (Dropbox, Google Drive) unless your organization's policy permits it.
- Lock your screen when you step away from your computer — even for a minute. Use a keyboard shortcut (Ctrl+L on Windows, Cmd+Ctrl+Q on Mac) to make it instant.

What to Do When Something Goes Wrong

The most important thing you can do when you suspect a security problem is **report it immediately.** Speed is everything. A reported incident can be contained in hours. An unreported incident can become a catastrophe over weeks or months.

Report These Things

- An email or message that looks like phishing — even if you're not sure
- A phone call asking for your password or account information
- Clicking a link or opening an attachment that you now suspect was malicious
- Your computer behaving strangely (unexpected pop-ups, slowness, programs you didn't open)
- Losing a device (laptop, phone, USB drive) that contains work information
- Discovering that you sent information to the wrong person
- Noticing someone accessing systems or information they shouldn't have access to

How to Report

Follow your organization's reporting procedure. If you don't know the procedure, ask your manager or IT department. The reporting process should be simple — if it's not, tell someone. A reporting process that's hard to use is a reporting process that doesn't get used.

You will not get in trouble for reporting. Organizations that punish employees for reporting security concerns get fewer reports — and more breaches. Your vigilance is valuable. Use it.

Working Remotely

If you work from home, from a hotel, or from a coffee shop, you're accessing your organization's systems from a network that isn't controlled or monitored by your IT department.

- **Use the VPN** if your organization provides one. The VPN encrypts your connection so that anyone on the same Wi-Fi network can't see your traffic.
- **Don't use public Wi-Fi for sensitive work** without a VPN. The coffee shop's Wi-Fi is convenient. It's also shared with everyone in the building.
- **Keep your home Wi-Fi secure.** Change the default password on your router. Use WPA3 if your router supports it (WPA2 at minimum). Don't use an open (unprotected) network.
- **Separate work and personal.** If your organization provides a work computer, use it for work. If you use a personal device for work, keep work files in the designated work environment (e.g., a managed container or virtual desktop) rather than mixing them with personal files.

AI Tools: What You Need to Know

AI tools (ChatGPT, Microsoft Copilot, Google Gemini, and others) are increasingly common in the workplace. They can be genuinely helpful — but they introduce risks you should understand.

- **Data you put in may not stay private.** When you paste text into an AI tool, the provider may retain it, use it for training, or surface it in responses to other users. Don't paste confidential information, customer data, patient records, or proprietary business information into AI tools unless your organization has specifically approved that tool and use case.
- **AI can be wrong.** AI generates responses that sound confident regardless of whether they're accurate. Don't rely on AI output for facts, figures, or decisions without verifying independently.
- **Follow your organization's policy.** Your organization should have a policy on which AI tools are approved and what data you can share with them. If there's no policy, ask — and err on the side of not sharing sensitive information until you have guidance.

The Three Things That Matter Most

If you remember nothing else from this guide, remember these:

1. **Pause before you click.** Most successful attacks depend on someone acting quickly without thinking. Ten seconds of thought can prevent a breach.
2. **Report anything suspicious.** You are not expected to know whether something is an attack. You are expected to report it so someone who does know can evaluate it. Report early, report often, report without hesitation.

3. **Your vigilance matters.** Security technology is important, but it has limits. You — alert, cautious, and willing to speak up — are the defense that attackers cannot automate around.

This guide is a companion to Guerilla Security: The Martial Art of Information Security *(revised 2026), which provides the full technical and governance treatment for security practitioners and program builders. Both are available at www.rescor.net.*