BITRALYNX
SOLUTIONS

FREE GUIDE

Why Antivirus Alone Is Not Enough Anymore

How attacks really get in during 2026, and the layers that keep your staff working and your services running

Bitralynx Solutions
Managed IT, cybersecurity, AI governance, and fractional CIO services for New York nonprofits and law firms
October 2026 | bitralynx.com

Start here

Antivirus is still worth having. It is a smoke detector for known bad files.

But a smoke detector does not stop a burglar who walks in with a key. And in 2026, many attackers walk in with a key. They get a real password, a real phone call, or a real remote access tool. No bad file is needed at all.

This guide explains how attacks work today, in plain words. It shows the layers that matter and what to ask your IT provider. You do not need to become an expert. You need the right questions.

> We are not here to scare you. Most of this is practical and fixable.

Why this matters for a nonprofit or a law firm

A nonprofit holds client records, donor details, and funder reports. A law firm holds privileged files. If your systems stop, people who count on you are affected. That is the real cost of an attack.

The numbers show why attackers care about smaller organizations too:

- The FBI's Internet Crime Complaint Center received 1,008,597 complaints in 2025. Reported losses were $20.877 billion, up 26 percent from 2024. [1]
- In Verizon's 2026 breach study, ransomware showed up in 48 percent of all breaches, up from 44 percent the year before. [2]
- The same study found that a human element, such as a click, a reused password, or a mistake, was present in 62 percent of breaches. [2]

PART 1

How attackers get in now

Door 1: Stolen logins

A login is a username and a password. Attackers get them in many ways. They buy them from earlier breaches. They trick people into typing them on fake pages. They also use "infostealer" programs. These quietly copy saved passwords from a computer.

Verizon found that credential abuse, which means using stolen logins, started 13 percent of breaches in its 2026 report. That is down from past years, when it was the top way in, but it is still a common door. [2] Sophos found compromised credentials behind 22 percent of the ransomware attacks in its 2026 U.S. survey. [6]

Once someone has a valid login to your email or cloud files, they look like a normal staff member. Antivirus has nothing to flag.

Door 2: Phishing, now with AI

Phishing is a fake message that tries to make you click, sign in, or pay. It used to be easy to spot. Bad spelling gave it away. Today, AI tools help criminals write clean, believable messages that fit your organization.

The FBI's 2025 report counted 22,364 complaints that involved AI, with about $893 million in reported losses. [1] Business email compromise, where a criminal poses as a boss or a vendor to redirect a payment, cost victims over $3 billion in reported losses in 2025. [1] Verizon found that generative AI helped with about 15 percent of the attack techniques in its 2026 report. [2]

Door 3: Fake IT help desk calls

This one is growing. An attacker calls your help desk, or your staff, and pretends to be someone else. They sound calm and friendly. They say they are locked out and need a password reset. Or they say they are IT and need to "fix a problem" on your computer.

A joint warning from CISA and the FBI, updated July 29, 2025, describes this method. Attackers pose as employees to convince help desk staff to reset passwords or move a

person's sign in codes to a device the attacker controls. [3]

Google's Mandiant team saw the same trend. Voice phishing, which means phishing by phone call, rose to 11 percent of the attacks they investigated in 2025. It became the second most common way in. [4]

> **Callout (a made up example):** Imagine a front desk worker at a counseling nonprofit gets a call. The caller says he is from IT and a "security alert" needs her to read back a code that just arrived on her phone. She is helpful, so she reads it. That code was the attacker's key to her email. Nothing was installed. No antivirus alarm rang. This story is made up, but the pattern is real.

Door 4: Voice cloning and deepfakes

Criminals can copy a voice from a short recording. In May 2025, the FBI warned about a campaign using AI generated voice messages to pose as senior officials and win trust. [5] The same trick works on your organization. A "call from the executive director" asking for an urgent payment may not be her at all.

The FBI's advice is simple. Verify the person using a number you already know. Agree on a code word with people you trust. Never share a sign in code with anyone. [5]

Door 5: Remote access tools

Remote desktop programs let IT staff fix computers from far away. Attackers love them for the same reason. If a staff member is tricked into installing one, the attacker controls the computer.

CISA's advisory notes that attackers abuse legitimate remote access software, and that this helps them get past security alerts, because the program is a normal, trusted application. [3] Antivirus often stays quiet because the software is not a virus.

Door 6: Unpatched systems that face the internet

A patch is a software update that fixes a known weakness. Attackers scan the internet around the clock for systems that have not been patched. This includes firewalls, VPNs (secure remote connections), and email servers.

Verizon's 2026 report found that exploiting weaknesses is now the most common way into a breach, at 31 percent. For small and medium sized businesses it was 26 percent. [2]

Mandiant's 2026 report found that exploits were the top way in for the sixth year running, at 32 percent. [4] Studies count differently. In Sophos's 2026 U.S. ransomware survey, phishing (27 percent) and malicious email (26 percent) led, and exploited weaknesses were 16 percent, down from 27 percent the year before. [6] The order changes by study, but weak spots and email tricks show up in all of them.

PART 2

Why many attacks never trip antivirus

Traditional antivirus compares files to a list of known bad files. Here is why it misses so much today.

No malware at all. If an attacker signs in with a real password, there is no bad file to find. The system sees a normal login.

Legitimate tools. Attackers use programs that are already on your computers, or trusted tools like remote access software. Security teams call this "living off the land." The tools are real, so they look harmless.

Cloud accounts. Much of your work now lives in Microsoft 365, Google Workspace, and other online systems. Antivirus watches individual computers. It does not watch a stranger signing in to your mailbox from another country.

Speed. Mandiant found that once one group breaks in, the median time to hand that access to another criminal group fell to just 22 seconds in 2025. In 2022 it was more than eight hours. [4] You cannot rely on someone noticing next week.

PART 3

Data theft and extortion, even without encryption

When most people hear "ransomware," they picture files locked and a ransom note. That still happens. But attackers have added another step. They copy your data first. Then they threaten to publish it or sell it.

CISA's ransomware guide describes this as "double extortion." It also warns that attackers may steal data and threaten to release it as their only form of extortion, with no locking of files at all. [7] CISA's Scattered Spider update says the group typically steals data for extortion, and sometimes also encrypts systems. [3]

Why this matters for you:

- Good backups help you recover locked files. They do not help if the threat is "we will release your client files."
- For a law firm, a leak can break client confidentiality. For a nonprofit, it can expose people who trusted you.
- Notice rules may apply even if nothing was locked. New York law requires businesses to notify affected New York residents within 30 days after discovering a breach. [8]

For scale: Verizon found the median ransom paid was $139,875, and 69 percent of ransomware victims did not pay. [2] Sophos found that U.S. organizations hit by ransomware, with 100 to 5,000 staff, spent an average of $2.51 million to recover, not counting any ransom. [6]

PART 4

The layers that matter

No single tool stops everything. The answer is layers. Each layer covers a gap the others leave open. Below, each layer is explained in plain words, with what to ask your IT provider.

Layer 1: Endpoint detection and response, watched around the clock

An "endpoint" is any computer or server. Endpoint detection and response (EDR) is the modern cousin of antivirus. It does not just match files. It watches what programs and users do, and it records activity so a specialist can look back and see what happened.

The key word is *watched*. A tool that sends alerts to a mailbox nobody reads at 2:00 AM helps no one. Many organizations pair EDR with a service where trained analysts watch alerts 24 hours a day, every day. This is often called managed detection and response.

Ask your IT provider:

- Who watches the alerts, and when? Is it a person or only an email?

Layer 2: Phishing resistant sign in

Two step sign in, also called multi factor authentication (MFA), asks for a second proof beyond a password. It is much better than a password alone. But not all second steps are equal.

Text message codes and phone call codes can be tricked or stolen. Attackers can send many "approve" prompts until a tired person taps yes. They can also trick someone into reading a code aloud, or swap a phone number to a different SIM card.

"Phishing resistant" sign in uses a passkey or a security key. These are tied to your real website and your real device. A fake page cannot use them. CISA's updated advisory says phishing resistant MFA is needed because it is not open to push bombing or SIM swap attacks. [3] CISA's ransomware guide recommends it for email, remote access, and any account that reaches critical systems. [7]

If you use Microsoft 365, note this: starting September 1, 2026, Microsoft made passkeys the default sign in setup for people who use text or voice codes in Microsoft Entra ID. Microsoft's own text and voice code delivery retires February 1, 2027 for most users. Global administrators and outside users follow July 1, 2027. After those dates, people whose only method is a text or voice code must register a passkey to keep signing in. Organizations that truly need text or voice codes can set up a separate phone provider. [9]

Ask your IT provider:

- Which of our accounts use passkeys or security keys, and which still use text codes?
- Is two step sign in required for everyone, including leaders, volunteers, and board members who use our systems?
- Are we ready for Microsoft's text and voice code changes?

Layer 3: Email security and DMARC

Most attacks still arrive by email, so the front door needs a strong lock. Email security tools scan links and attachments, catch fake login pages, and flag messages that pretend to be from someone in your organization.

DMARC is a setting for your own domain name. It tells the world how to treat email that claims to come from you but did not. Without it, anyone can send mail that looks like it is from your executive director. With it set up properly, fake mail can be blocked or sent to spam by the receiving side.

DMARC has also become an expectation for senders. Since February 2024, Google has required large senders to set up DMARC. [10] It also protects your name with donors, clients, and partners.

Ask your IT provider:

- Is DMARC set up for our domain? Is it only in "monitor" mode, or does it actually block fake mail?

Layer 4: Patching and replacing old systems

Patching means installing updates that fix known weaknesses. It is boring, and it is one of the most effective things you can do. The numbers above show why: attackers go straight for weak spots that are known and not yet fixed.

Watch end of life dates, too. Windows 10 reached end of support on October 14, 2025. After that date, a computer on Windows 10 no longer gets security fixes, unless it is enrolled in Microsoft's paid Extended Security Updates program. [11] Those programs are a bridge, not a plan. Replacing or upgrading those computers is the plan.

Ask your IT provider:

- Do we have any computers, servers, or devices that no longer get security updates?

- How fast do you patch the most serious problems, especially on firewalls and remote access?

Layer 5: Backups that cannot be changed

Backups are your recovery plan. But attackers know this. CISA warns that many ransomware attackers try to find and delete or lock your backups first. [7] A backup copy that sits on the same network as everything else can be wiped along with it.

A strong setup keeps at least one copy that is offline or "immutable." Immutable means it cannot be changed or deleted for a set time, even by someone with an administrator login. CISA recommends encrypted, offline backups, and a recent advisory also names immutable, separately stored backups that are tested regularly. [3][7] CISA adds one caution: immutable storage can conflict with some compliance rules, so choose it with care. [7]

Testing matters as much as the backup. A backup you have never restored is a hope, not a plan.

Ask your IT provider:

- Is at least one copy of our backups offline or immutable?
- When did we last do a real test restore, and how long did it take?

Layer 6: Staff training that matches today’s tricks

Keep training short, regular, and kind. Nobody should feel foolish for reporting a mistake. Cover phone calls and fake IT requests, and teach these habits:

- If someone asks for a code, a password, or a payment change, stop and check using a known phone number.
- IT will never ask you to read a sign in code aloud.
- Agree on a code word for urgent requests from leaders.
- Report odd calls and messages right away.

Ask your IT provider:

- How often is training done, and does it cover phone calls and AI generated fakes?

Layer 7: Fewer admin rights

An "administrator" account can install software and change settings. If an attacker takes over an administrator account, they can take over everything. So keep those accounts few and protect them well.

Each person gets only the access they need. Administrators use a separate account for admin work and a normal one for email and web. CISA's ransomware guide recommends exactly this. [7] This also helps with the help desk trick.

Ask your IT provider:

- How many people have administrator rights, and why?
- Do administrators use a separate account for everyday work?
- What identity checks does the help desk do before resetting a password or changing someone's sign in method?

Layer 8: A written response plan

When something goes wrong, minutes count. A written plan answers in advance: Who do we call first? Who decides to shut systems off? Who talks to clients, funders, or the media? When do we call a lawyer or our insurer?

CISA advises creating a basic response plan, practicing it, and keeping a paper copy and an offline copy. [7] For a nonprofit, add funder and regulator notice. For a law firm, add duties to clients and your professional liability carrier. For organizations that handle health information, the HIPAA Security Rule already requires safeguards today. A proposal to update that rule was published in January 2025. As of our latest check, we found no final rule, and the federal regulatory agenda lists final action for July 2027. Dates like that can move. [12]

Ask your IT provider:

- Do we have a written response plan, and when was it last practiced?
- Does it include our insurer's hotline and our legal contacts?

Layer 9: Cyber insurance, and what it asks of you

Cyber insurance helps pay for recovery, and insurers often ask questions first. Insurers commonly ask about things like two step sign in, EDR, tested backups, and a written response plan.

Requirements differ by insurer, so read your own application. Answer honestly. A claim can be denied if a form says you have a control you do not really have.

Ask your IT provider:

- Which controls does our cyber insurer ask about, and can we show them?

PART 5

Where to start

You cannot do everything this month. Start with the doors that matter most.

- **This week:** Turn on two step sign in for every email and cloud account. End password reuse. Agree on a code word for urgent phone requests.
- **This quarter:** Move leaders and administrators to passkeys. Confirm EDR is on every device and someone watches it. Check DMARC. Do one real test restore. Write down the response plan.
- **This year:** Replace systems that no longer get updates. Review administrator rights. Refresh training. Review insurance questions with your broker.

Questions to ask your IT provider

Print this page. Bring it to your next meeting. A good provider will welcome these questions.

- [ ] Do we run EDR on every computer and server, and who watches the alerts around the clock?
- [ ] Which accounts use passkeys or security keys, and which still use text or voice codes?

- [ ] Is two step sign in required for every staff member, leader, and outside user?
- [ ] Are we ready for Microsoft's text and voice code changes?
- [ ] Is DMARC set to actually block fake mail from our domain?
- [ ] Which devices or systems no longer get security updates, and what is the plan for them?
- [ ] How fast are serious problems patched on firewalls and remote access?
- [ ] Is at least one backup offline or immutable, and when did we last test a restore?
- [ ] Who has administrator rights, and do they use separate accounts?
- [ ] What identity checks happen before a password reset or sign in change?
- [ ] Does training cover phone calls, fake IT requests, and AI voices?
- [ ] Do we have a written response plan that names who does what, and has it been practiced?
- [ ] Which controls does our cyber insurer ask for, and can we prove them?

Sources

1. FBI Internet Crime Complaint Center, 2025 Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
2. Verizon, 2026 Data Breach Investigations Report (data from Nov 1, 2024 to Oct 31, 2025) and Executive Summary. https://www.verizon.com/business/resources/reports/dbir/ and https://www.verizon.com/business/resources/executivebriefs/2026-dbir-executive-summary.pdf
3. CISA and FBI, Scattered Spider advisory AA23-320A (updated July 29, 2025). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a
4. Google Mandiant, M-Trends 2026. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026 and https://cloud.google.com/security/resources/m-trends-executive-edition (coverage read: https://www.helpnetsecurity.com/2026/03/24/mandiant-m-trends-2026-report/)
5. FBI, Public Service Announcement I-051525-PSA, May 15, 2025. https://www.ic3.gov/PSA/2025/PSA250515
6. Sophos, The State of Ransomware in the U.S. 2026 (July 2026, 377 U.S. organizations with 100 to 5,000 staff, all hit by ransomware). https://assets.sophos.com/X24WTUEQ/at/tsttpn5wtvfzjw7f4cn89/sophos-state-of-ransomware-in-us-2026.pdf
7. CISA, #StopRansomware Guide. https://www.cisa.gov/stopransomware/ransomware-guide
8. New York General Business Law section 899-aa (statute text). https://www.nysenate.gov/legislation/laws/GBS/899-AA
9. Microsoft Learn, Passkeys by default and retirement of Microsoft provided SMS and voice authentication (page dated September 23, 2026). https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sms-voice-retirement
10. Google, Email sender guidelines. https://support.google.com/a/answer/81126
11. Microsoft Learn, Extended Security Updates (ESU) program for Windows 10. https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates
12. Office of Information and Regulatory Affairs (reginfo.gov), Unified Agenda entry for the HIPAA Security Rule update (RIN 0945-AA22). https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22 and proposed rule, Federal Register, Jan 6, 2025: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information

NEXT STEP

Talk it through with us

Bitralynx Solutions offers a free 30 minute Technology Readiness Review. It is a conversation, with no access to your systems needed. Bring this guide and your questions. You leave with a short list of what is solid and what to fix first.

Keep your staff working and your services running.

info@bitralynx.com | (516) 855-5353 | bitralynx.com/how-we-start

This guide is general information for nonprofit and law firm leaders. It is not legal advice, a security certification, or a full risk assessment. Facts were checked in October 2026; threats and rules change, so confirm current guidance before you act. Bitralynx Solutions is an IT company, not a law firm.