

CYBERSECURITY AWARENESS MONTH

Don't Make It Easy for Them: Four Habits That Make Your Business a Harder Target

The best way to mark Cybersecurity Awareness Month isn't a big purchase. It's a few small habits, done consistently.

Every October, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance lead Cybersecurity Awareness Month. CISA's 2026 theme is "Securing the Next 250," and the Alliance's is "Don't Make It Easy for Them."^{1,3} The message is the same: simple, steady habits stop most attacks.

The need is real, and it's close to home. In the FBI's 2025 Internet Crime Report, Texas ranked second in the nation for cybercrime complaints and for reported losses.⁴

#2 in the U.S.

Texas in 2025: 97,912 complaints and about \$1.8 billion in reported losses to the FBI's IC3.⁴

Most attacks on small businesses don't start with a genius hacker. They start with a reused password, a missed update, or a convincing email on a busy afternoon. CISA's four core steps close exactly those gaps:²

- 1 Recognize and report phishing.** Teach staff to pause before clicking, and make it easy to forward anything suspicious.
- 2 Use strong passwords.** Long, unique passphrases for every account, kept in a password manager instead of on a sticky note.
- 3 Turn on multifactor authentication (MFA),** starting with email, banking, and Microsoft 365 or Google Workspace.
- 4 Update software.** Turn on automatic updates, and replace computers and equipment that no longer get security fixes.

CISA also urges organizations to back up their data and keep an incident response plan, even a one-page list of who to call and what to do first.²

None of this is glamorous, and that's the point. Pick one step this month, finish it, then move to the next. If you'd like a second set of eyes, we're happy to walk through it with you, and we can come to you.

⚠️ SCAM OF THE MONTH

[SHARE THIS WITH YOUR STAFF](#)

The "We Changed Banks" Email, Now With a Phone Call That Sounds Real

It looks routine: a vendor, a client, or even your own boss emails to say their bank details changed and asks you to update them before the next payment. It may come from the *real* account, because that mailbox was hacked. A follow-up call or voicemail may "confirm" it, and AI voice cloning can make the caller sound like someone you know.⁴

This is **business email compromise (BEC)**. In 2025, the FBI's IC3 received 24,768 BEC complaints with about \$3 billion in reported losses, second only to investment fraud.⁴

RED FLAGS

- New or changed bank account or payment instructions
- Urgency or secrecy: "I'm in a meeting, just handle it"
- A sender address or reply-to that is slightly off
- A push to move to text or personal email

WHAT TO DO

- **Call back using a number you already have on file,** never the one in the email.⁵
- Have a second person approve payment changes.
- If money went out, call your bank right away to request a recall, then report it at **ic3.gov**.⁵

CHECKLIST

3 Quick Wins This Month

- ☐ **Write a “payment change” rule.**
Any new or changed bank details get verified by phone using a number already on file, and approved by a second person. Post it where your billing staff can see it.
- ☐ **Confirm MFA is on for every email account.**
That includes the owner, the office manager, and anyone who handles payments or patient and client records.
- ☐ **Test one restore.**
Pick an important file or folder and restore it from backup. A backup you’ve never tested is only a hope.

Pass it along: print this issue for the break room or forward it to your team. The Scam of the Month on page 1 is written for front-desk, billing, and bookkeeping staff, the people most likely to see payment requests.

ASK THE TECH

Our Windows 10 PCs still work. Do we need to replace them?

Q: We still have a couple of Windows 10 computers at the front desk. They run fine. Is that a problem?

A: Probably, yes. Windows 10 reached end of support on October 14, 2025. Since then, Microsoft sends security fixes only to Windows 10 PCs enrolled in its Extended Security Updates (ESU) program.^{6,7}

For business PCs, the first ESU year ends **October 13, 2026**.⁶ If your PCs are enrolled, make sure the second year is in place. If they aren’t, those computers haven’t received security fixes in about a year, which makes them an easy way in.

The long-term fix is Windows 11: upgrade the PCs that meet its requirements and plan to replace the ones that don’t. Not sure which machines are still on Windows 10? Call us at (806) 319-8521 and we can help you take inventory.

Services for West Texas Businesses

Double Technologies offers these services to businesses across Lubbock and West Texas. Each one now has its own plain-language page on our website:

- Help Desk & On-Site Support
- Managed Firewall & Security Monitoring
- Email Security
- Security Awareness Training
- Vulnerability & Pen Testing
- Cloud Services
- Co-Managed IT
- Cyber Insurance & Compliance

Learn more at doubletechnologies.com, or call (806) 319-8521 to talk with our team.

Have questions? Call (806) 319-8521 or visit doubletechnologies.com to talk with our team.

DOUBLE TECHNOLOGIES

Managed IT & Cybersecurity · Lubbock, Texas
30 years of combined experience. Serving Lubbock, Wolfforth, Levelland, Brownfield, Lamesa, Littlefield, Post, Plainview, Amarillo, Abilene, Midland, Odessa, and West Texas.

CONTACT

Phone: **(806) 319-8521**
Email: admin@doubletechnologies.com
Support: support@doubletechnologies.com
Web: doubletechnologies.com

HOURS (CENTRAL)

Monday–Friday: 8 AM–7 PM
Saturday: 9 AM–5 PM
On-site visits available. We can come to you.

Sources (accessed October 11, 2026). This newsletter is general information, not legal or insurance advice.

1. CISA, “CISA Launches Cybersecurity Awareness Month: Securing the Next 250,” Oct. 1, 2026. cisa.gov/news-events/news/cisa-launches-cybersecurity-awareness-month-securing-next-250
2. CISA, Cybersecurity Awareness Month (core steps and organizational steps). cisa.gov/cybersecurity-awareness-month
3. National Cybersecurity Alliance, “The National Cybersecurity Alliance Launches the 23rd Annual Cybersecurity Awareness Month,” Oct. 1, 2026 (GlobeNewswire).
4. FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report, April 2026: state rankings, BEC, and AI sections. ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
5. FBI IC3, Public Service Announcement “Business Email Compromise: The \$55 Billion Scam,” Sept. 11, 2024. ic3.gov/PSA/2024/PSA240911
6. Microsoft Learn, “Product Lifecycle FAQ: Extended Security Updates” (Windows 10 ESU year dates). learn.microsoft.com/lifecycle/faq/extended-security-updates
7. Microsoft Learn, “Extended Security Updates (ESU) program for Windows 10.” learn.microsoft.com/windows/whats-new/extended-security-updates