DOUBLE TECHNOLOGIES

CYBERSECURITY MONTHLY

NOVEMBER 2026 | HOLIDAY SEASON SECURITY

Practical IT and cybersecurity tips for West Texas businesses

doubletechnologies.com · (806) 319-8521

RANSOMWARE ALERT

A New FBI Ransomware Warning, and Four Checks to Make Before the Holidays

The group behind it gets in the ordinary way: weak passwords and equipment that hasn't been updated.

On October 20, CISA, the FBI, the U.S. Secret Service and international partners issued a joint warning about SafePay, which they call one of the most active ransomware groups of 2026.[1,2]

~600 victims

About 600 organizations hit by SafePay ransomware since August 2024, across the Americas, Europe and Australia.[1,2]

How they get in isn't exotic: stolen or guessed passwords, phishing, and known flaws in internet-facing equipment like firewalls and VPNs, the devices that let staff connect from outside the office.[1]

Once inside, they use normal IT tools to move around, delete or disable backups, steal data, and then lock up files and demand a ransom. Sometimes they even call victims directly to pressure them.[2]

The holidays are a good time to check your defenses, before staff take time off and fewer people are watching. The agencies' advice comes down to four steps:[1,2]

1. **Update firewalls, VPNs and other internet-facing equipment first.** Firmware counts, not just Windows.
2. **Require multifactor authentication (MFA),** especially for remote access and email.
3. **Keep at least one backup offline,** and test that you can restore from it.
4. **Limit admin rights.** Everyday accounts shouldn't be able to change systems.

None of these steps requires buying anything new. Each one just needs someone to own it. If you're not sure where your business stands, call us at (806) 319-8521. We'll walk through it with you, and we can come to you.

⚠ SCAM OF THE MONTH

SHARE THIS WITH YOUR STAFF

"Your Package Is on Hold": Fake Delivery and Customs-Fee Texts

It's peak shipping season, and scammers know it. A text or email that looks like it's from USPS, UPS or FedEx says a package can't be delivered until you confirm your address or pay a small fee. A newer twist claims the order is "stuck in customs" until you pay a tariff.[3]

The link leads to a fake site that steals card numbers and personal information, or downloads malware onto your device.[4] Offices that order supplies all season are easy targets, and one click on a work phone or computer can put business accounts at risk.

RED FLAGS

- A notice for a package you don't remember ordering
- A fee to release or redeliver a package
- A deadline: "returned unless you act today"
- A link that doesn't match the carrier's real website

WHAT TO DO

- **Don't click or reply.** Check tracking on the carrier's or seller's website yourself.[3]
- Forward suspicious texts to **7726** (SPAM).[3]
- If you entered card details, call your bank or card company right away, then report it at **ReportFraud.ftc.gov**.[6,7]

CHECKLIST

3 Quick Wins This Month

- [ ] **Make a "no gift cards" rule.**
  Tell staff the business never asks anyone to buy gift cards by text, email or phone. If the "boss" asks, check using a number you already know.[5]
- [ ] **Make sure one backup is offline.**
  Ransomware crews go after backups first. Keep at least one copy disconnected from your network, and test a restore.[1,2]
- [ ] **Turn off old accounts.**
  Disable logins for former employees and seasonal help, and remove admin rights from accounts that don't need them.[1]

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 anyone who orders supplies or receives packages at the office.

ASK THE TECH

Should we let staff shop online on work computers?

Q: It's that time of year, and some of our team shops online during lunch. Is that a problem?

A: It's your call, but set a few ground rules. The FBI warns that holiday shoppers lose money to fake sellers, gift card payment requests and deals that are too good to be true. In 2025, non-payment and non-delivery scams cost victims more than $503 million.[6]

Ask staff to shop only on sites they type in themselves, never from links in texts or emails, and to pay with a credit card so a bad charge is easier to dispute.[6] Keep personal shopping off the business email address, too.

Above all, keep work computers updated, since a fake shopping site is one more way in. Want help writing a simple policy? Call us at (806) 319-8521.

New on Our Website

We've added plain-language pages to help businesses across Lubbock and West Texas find what they need:

- AI Security
- AI Services & Microsoft Copilot Setup
- Law Firm IT & Cybersecurity
- About Double Technologies
- IT Services in Amarillo
- IT Services in Abilene
- IT Services in Midland & Odessa
- IT Support Across the South Plains

Find them 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**
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 November 1, 2026). This newsletter is general information, not legal or insurance advice.

1. CISA, FBI, U.S. Secret Service and partners, "#StopRansomware: SafePay Ransomware," Advisory AA26-293A, Oct. 20, 2026. cisa.gov/news-events/cybersecurity-advisories/aa26-293a
2. CISA, "CISA, FBI and Partners Warn Organizations of SafePay Ransomware Actors Targeting Multiple Critical Infrastructure Sectors," Oct. 21, 2026, and CISA bulletin on the joint advisory. cisa.gov/news-events/news
3. Federal Communications Commission, "How to Identify and Avoid Package Delivery Scams." fcc.gov/how-identify-and-avoid-package-delivery-scams
4. Better Business Bureau, "How to Spot and Avoid Delivery Scams." bbb.org/scams/delivery-scams
5. FTC Consumer Advice, "No, That's Not Your Boss Asking You to Buy Gift Cards," Jan. 2026. consumer.ftc.gov/consumer-alerts/2026/01
6. FBI, "Holiday Scams" (cites the IC3 2025 report). fbi.gov/how-we-can-help-you/common-frauds-and-scams/holiday-scams
7. FTC Business Blog, "As Holiday Shopping Begins, the FTC and IRS Agree: Scams and Identity Theft Are Always Bad for Business," Dec. 2024. ftc.gov/business-guidance/blog