Mirazon®
Providing Vision for Technology Solutions

Holiday Cyber Survival Guide

'Tis the Season… for Scammers?

Between the shopping sprees, travel plans, and endless "limited-time offers," the holidays are prime time for cybercriminals. Scammers know you're busy—and they're counting on it. From fake delivery alerts to too-good-to-be-true deals, their goal is simple: catch you off guard.

But don't worry—Mirazon's got your back. Here's your quick-read five-point guide to staying safe, secure, and scam-free this season.

Treat every "urgent" link like a red flag.

Those "Your delivery can't be made" or "Your account has been compromised" messages are some of the most common holiday scams. The IRS warns that fraudsters often pose as legitimate organizations—like shipping companies, banks, or even the IRS itself—to trick you into clicking malicious links or sharing personal info.

Tip: Don't take the bait. Instead of clicking, go directly to the official website or app to check your account or shipment status. When in doubt, delete it out.

Gift cards ≠ safe payment.

Scammers love gift cards because once the money's gone—it's gone. The AARP reports that nearly one in three consumers have received a gift card that turned out to have no balance. Fraudsters are posing as charities, tech support, or even friends to convince you to send codes as "payment" or "donations."

Tip: Only buy gift cards from trusted retailers, and in person whenever possible. Never share card numbers or codes over the phone, by email, or via text—especially with anyone demanding immediate payment.

Shopping deals that look too good often are.

It's the season of savings—but cybercriminals know that too. Fake online stores and social media ads are running rampant, promising luxury items or electronics at suspiciously steep discounts. According to ACAMS Today, these bogus sites are increasingly sophisticated, mimicking real retailers down to the last pixel.

Tip: Before checking out, double-check the site's URL (look for "https://" and a padlock). Read reviews from multiple sources. And when paying, use a credit card rather than a debit card—credit cards offer stronger fraud protections and dispute rights.

Ho Ho Hold up—and enable MFA.

It's the gift that keeps on giving: multi-factor authentication (MFA). Microsoft's research shows MFA can block over 99% of automated account takeover attempts. It adds a quick second step—like a text code or app notification—to make sure it's really *you* logging in.

Tip: Turn on MFA for every account that offers it—shopping, streaming, social media, everything. It's one of the easiest and most effective ways to lock down your digital sleigh.

Keep your devices and Wi-Fi secure.

Public Wi-Fi is convenient, but it's also a playground for cyber snoops. The IRS cautions against shopping or banking over unsecured networks, which make it easy for hackers to intercept your information. Combine that with an outdated device, and you've basically left cookies and milk out for scammers.

Tip: Update your devices this week (yes, even that one you "never use"). Skip the free café Wi-Fi for financial transactions—use your mobile hotspot instead. And if you haven't already, secure your home Wi-Fi with a strong password.

Cybercriminals don't take holidays, but with a few smart habits, you can keep your data and your wallet safe all season long. Stay alert, stay updated, and remember: if something feels off, it probably is.

From all of us at Mirazon, happy holidays and happy, secure shopping!

Mirazon®

Contact Us