Hacked for the Holidays

Gifts & Grifts

The holidays bring gifts, gatherings and gadgets — but they also bring an annual surge in cybercrime. According to the FBI's Internet Crime Complaint Center, reported scams spike by nearly **30% between November and January**. Here's how to protect yourself without killing the festive mood.

UMass Boston | Information Security Office

Toy drops & online shopping traps

Hype = Hacker Opportunity

Limited-stock toy releases and livestream "drops" create urgency — and urgency makes people lower their guard. Scammers know this and use realistic websites, bogus promo codes and fake resale listings to trick buyers into sending them money for nothing.

Common dangers:

- "Exclusive access" links sent through social media or text
- Copycat sites with slight domain changes (like .shop or .store versions)
- Deep discount listings requiring payment through apps or gift cards

Smart moves:

☑ Go directly to the retailer's official website or app
☑ Be suspicious of "one-time" 50–90% discounts
☑ Avoid buying through links shared in comments or DMs

A 2023 BBB report found that over 75% of victims of online purchase scams never received the product they ordered.

Smartwatches: Convenient but vulnerable

Smartwatches now store health data, contacts, messages and login credentials — and many don't rely solely on your phone for internet access.

What can go wrong:

- Wi-Fi connections outside your phone's VPN protection
- Outdated software lacking basic patches
- Malware downloads via insecure networks

Reduce the risk:

☑ Keep the watch paired to your phone
☑ Use a VPN on your phone so the watch routes through it
☑ Turn off auto-join for unknown Wi-Fi networks
☑ Update both the watch and app regularly

Security analysts at Kaspersky estimate that **1 in 4 wearable devices** connect to unsecured networks at least once a week.

Shared Wi-Fi, shared risks

When guests arrive, so do their devices — and not all of them are secure. Even one outdated tablet or infected phone can expose your entire home network to risk.

Good digital housekeeping:

☑ Update your own devices before company arrives
☑ Turn on your router's VPN if available
☑ Only share the Wi-Fi password with people you know
☑ If possible, create a guest network to isolate traffic

Unpatched devices are a common threat — CISA reports that **over 60% of malware infections exploit outdated software**.

Final thoughts

You don't need to unplug to stay protected — you just need to stay aware. With a few proactive steps, you can shop, stream,

Quick cyber-check

Before the party starts, take these five steps:

1. Stick to authorized online sellers

2. Double-check unfamiliar URLs and "flash sale" links

3. Pair wearable tech securely through your phone

4. Update devices ahead of gatherings

5. Use router-level security when you can

INFOSEC