SHARED DEVICES = SHARED RISK

The holidays bring convenience: new devices, shared tablets, family laptops, and quick logins so everyone can shop, stream, or just check things on the go. While shared devices can make life easier, they can also quietly increase the risk of fraud – or at the very least, expensive surprises.

Shared devices are especially common this time of year. Phones get handed to kids, tablets stay logged in for family use, and cards are saved to avoid typing the same information over and over again. Most of the time, nothing happens… until it does.

WHAT IS THE RISK?

When multiple people use the same device, safeguards tend to loosen. Accounts stay logged in. Payment details remain saved. Alerts are dismissed because it's assumed a family member made the purchase. And kids, being kids, click buttons without realizing there's real money attached.

REAL WORLD EXAMPLE: Years ago, my kid managed to purchase three full seasons of Rusty Rivets on Amazon Prime –one episode at a time. There was no fraud, no hacker, no scammer involved. Just a shared device, a saved payment method, and a curious child who didn't know better. Ouch.

Now imagine that same setup – saved cards and logged-in accounts – paired with a malicious pop-up, fake ad, or convincing method. This is where fraud enters the picture - fraud doesn't always start with a breach or a criminal breaking into a system. Often, it starts with unintended access on a device that's already trusted.

WHY DOES THIS RISK INCREASE DURING THE HOLIDAYS?

The holidays create the perfect storm:

- More purchases than usual
- More people using the same devices
- More notifications that can be easy to overlook or ignore
- Less time and energy to double–check activity

Scammers know this and they rely on distraction and assumption. If one small charge goes unnoticed or someone thinks, "That must've been one of us," fraud can linger much longer than it should.

HOW DO YOU STAY SAFE THIS SEASON?

A few small steps can significantly reduce your risk:

- Log out of banking, shopping, and payment apps when you're finished.
- Avoid saving credentials and payment details on shared devices whenever possible.
- Turn on transaction alerts so activity is seen immediately
- Use separate profiles or parental controls for children and guests
- Review unexpected notifications instead of just dismissing them

Shared devices don't have to mean shared risk – but they do require a little extra attention. Because, whether it's three seasons of a cartoon or something far more serious, a little prevention now can save a lot of frustration later.