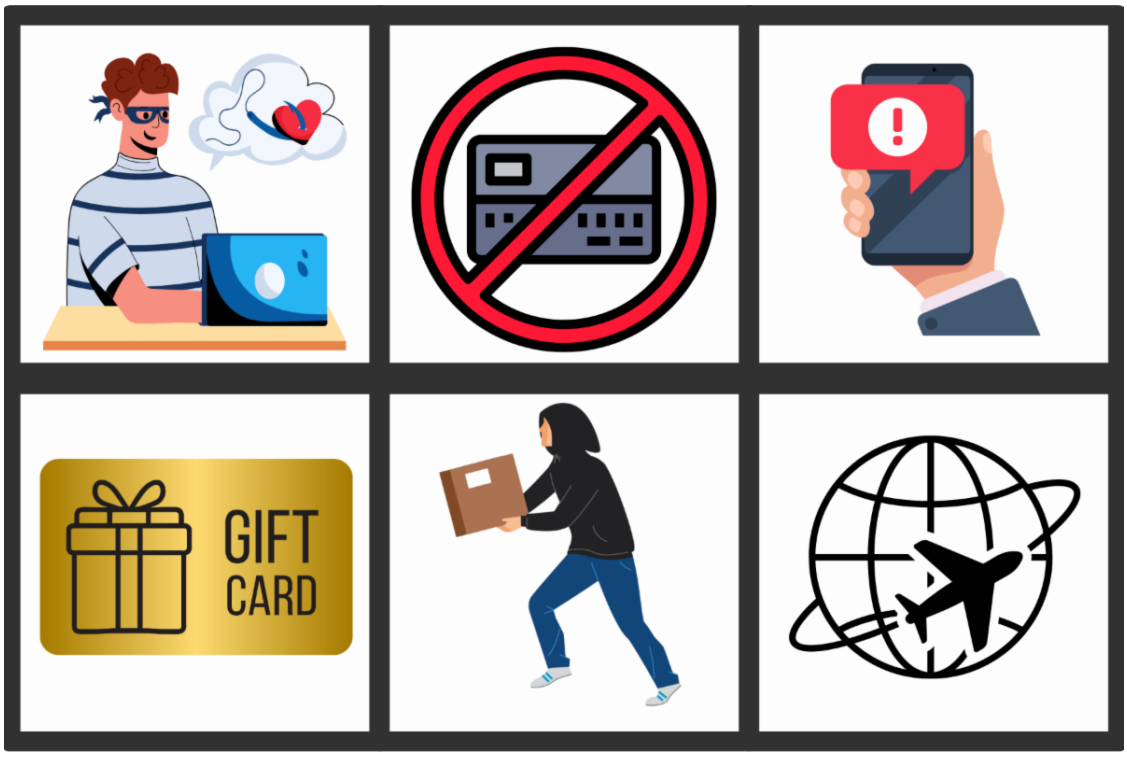
’Tis the Season to Be Cybersecure

With the holiday season upon us, cybercriminals ramp up their attacks hoping to catch consumers off guard. This year, however, their attacks may be aided by AI and more difficult to spot. The IBA has collected best practices and common scams to be aware of. Share this information with your consumers to help them and your bank stay safe. In this case, more knowledge equals better security, and that’s a gift everyone can use.

General Holiday Awareness Tips

- **Treat every email and advertisement with suspicion.** Don’t respond to unsolicited emails that ask you to click on a link or download an app to access a deal. Rather than clicking on a link from an email or text, go directly to the site of the company purportedly offering the deal. Watch out for spelling errors or incorrect grammar on email or text as these are typical red flags that help identify bogus content.
- **Is it too good to be true?** Look out for huge discounts on gift items, especially on social media posts or unfamiliar websites. These types of scams will impersonate major brands or nonexistent retailers to entice you with great deals for products you'll never receive.
- **Steer clear of Wi-Fi woes.** Avoid conducting any business online (making a purchase, donating, accessing password-protected sites) while using a public Wi-Fi network unless you employ a virtual private network (VPN).
- **Avoid peculiar payment methods.** Any time you are prompted to make a purchase or donation by wire transfer, cryptocurrency or gift card, it’s a scam.



Trending Scams

- **Charity scams:** Bogus charities exploit seasonal goodwill via fake websites, door-to-door solicitations and telemarketing. Pushy charity telemarketers could be an indicator

that they are imposters. Legitimate charities will accept your donations on your timeline. Be sure to do your research before you donate.

- **Credit card decline scams:** It's always a great idea to pay for gifts by credit card because you can dispute charges and limit the damage if the transaction was fraudulent. However, this new scam declines your credit card then asks for a second card. You'll be charged for purchase on both cards. If your purchase declines initially — and you believe it should not — don't provide a second card, contact the card issuer of the initial card instead.

- **Delivery scams:** During the gift-giving season, people are buying online and sending gifts. Beware of phishing emails from fraudsters posing as UPS, FedEx, U.S. Postal Service (USPS), or U.S. Customs and Border Protection. They also send messages (SMS/MMS), so be wary of content on your phone as well.

- **Gift card scams:** Criminals steal the numbers off gift cards from a rack in a busy grocery store or big box retailer. Once you load money onto the card, it gets siphoned off. Buy gifts cards online, instead of from a retail rack, where the cards can be tampered with. When receiving a gift card as a present, register it if that's an option, and use it sooner rather than later.

- **Porch pirates:** With holiday shopping and shipping comes package theft. In 2023, an estimated 3 in 4 Americans experienced package poaching. To outsmart porch pirates, retrieve a package as soon as it arrives. Have the sender require a signature, if possible. Also consider picking up your package somewhere else, such as shipping to your nearest store or your workplace.

- **Travel scams:** Criminals may use emails, texts or spoofed websites offering travel deals, such as free or heavily discounted tickets or travel packages, to get credit card information or download malware. To protect yourself from travel scams, determine if a website is real. Don't trust phone numbers as they can be easily spoofed. Also, be wary of travel businesses that ask for payment before confirming reservations.

Source: Iowa Bankers Association