



HOLIDAY PHISHING SCAMS

The holiday season is one of the busiest times of the year for online shopping, shipping, and charitable giving. Unfortunately, it's also one of the busiest times for scammers.

Criminals know people are expecting packages, hunting for deals, and making purchases online, making it easier for phishing scams to blend in with legitimate communications.

**DON'T LET FRAUDSTERS
STEAL YOUR HOLIDAY CHEER!**



HELPFUL TIP!

If you ever receive a suspicious message claiming to be from the bank, do not click links or provide account information.

Contact Citizens Bank Minnesota directly using a phone number from our website, a recent statement, or the back of your debit card.



FAKE HOLIDAY DEALS

If a deal seems too good to be true, it probably is.

Fraudsters create fake websites and social media advertisements promoting deeply discounted electronics, toys, gift cards, and other popular holiday items.

Once payment is made, the item never arrives, or the website captures your payment information.

Citizens

BANK MINNESOTA

Member FDIC



PACKAGE DELIVERY SCAMS

You receive a text message saying your package is delayed or cannot be delivered until you pay a small fee. The message includes a convenient link to "fix" the problem.

The link often leads to a fake website designed to steal your personal information, login credentials, or payment card details.

STAY SAFE:

Track packages directly through the retailer or shipping company.

Avoid clicking links in unexpected text messages.

Verify shipping updates through official websites or mobile apps.

GIFT CARD SCAMS

One of the biggest red flags in fraud is being asked to pay with gift cards.

No legitimate business, government agency, utility company, or bank will demand payment using gift cards.

If someone insists on gift card payment, it's almost certainly a scam.



PROTECT YOUR INFORMATION WHILE SHOPPING

- Shop with trusted retailers.
- Look for secure websites beginning with "https."
- Use credit cards or secure digital payment methods when possible.
- Avoid making purchases on public Wi-Fi networks.
- Review account statements regularly for unauthorized transactions.



STOP • VERIFY • PROTECT

Before responding to an email, text, phone call, or social media message, ask yourself:

Was I expecting this communication?

Is the sender who they claim to be?

Can I verify this request through a trusted source?

A few extra moments spent verifying a message could save you from becoming a victim of fraud.