CITIZENS FRAUD UPDATE

WHAT IS MAGECART?

Its a form of digital skimming in which cybercriminals inject malicious JavaScript into e-commerce checkout pages to steal credit card data directly from a shopper's browser. Protecting yourself means using secure browsing habits as a consumer and strong client-side security controls if you run an online store.
Below is a clear, structured breakdown of what Magecart is and how both shoppers and website owners can defend against it.

HOW IT WORKS

Magecart refers to multiple cybercriminal groups that steal payment card data by injecting malicious scripts into online checkout pages. Originally tied to the Magento platform, these attacks now target nearly every major e-commerce system.
How Magecart Works

• Attackers exploit vulnerabilities in a website or a third-party script (analytics, chat widgets, A/B testing tools, etc.).

• They inject a hidden JavaScript "skimmer" into the checkout page.

• When a shopper enters payment details, the script silently copies the data and sends it to the attacker—while the real transaction still goes through, making the theft hard to detect.

• Some groups even create fake payment forms or redirect users to look-alike checkout pages.

HOW TO PROTECT YOURSELF AS A SHOPPER

While consumers can't fully prevent a compromised website, you can reduce your risk:

✅ **USE VIRTUAL OR SINGLE-USE CARD NUMBERS**
Many banks and payment providers offer temporary card numbers that limit exposure if stolen.

✅ **PREFER DIGITAL WALLETS**
Apple Pay, Google Pay, and PayPal don't expose your actual card number to the merchant.

✅ **KEEP YOUR BROWSER & EXTENSIONS CLEAN**
Malicious extensions can also skim data. Stick to trusted extensions and update your browser regularly.

✅ **MONITOR YOUR STATEMENTS**
Magecart attacks often go unnoticed for weeks. Early detection helps you dispute fraudulent charges quickly.

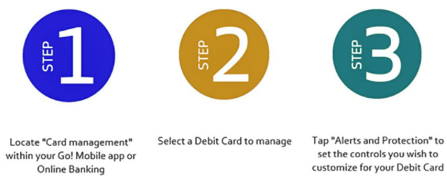
✅ **AVOID ENTERING CARD DATA ON SUSPICIOUS OR OUTDATED SITES**
If a checkout page looks broken, loads slowly, or behaves strangely, back out.

Added Security at your Fingertips

CARD MANAGEMENT

Take full control of your *Citizens Bank Minnesota* Debit Card right from your Go! Mobile app!

Our powerful, portable app offers advanced Debit Card controls that allow you to safely and securely manage your money. It's as easy as 1-2-3 to set alerts and restrictions on your Debit Card(s), just follow the instructions below!



All Debit Cards associated with accounts linked within your Online Banking will be available within Card Management.

Card Management options:
• Toggle to lock and unlock your Debit Card in real time.
• Within Alerts and Protections, manage your notification settings to be alerted via text message, e-mail, or in-app messages for blocked transaction and notification alerts.
• Protection options allow you to toggle on and be alerted for all Debit Card transactions.
• Additional customization available for Locations, Merchant Types, Transaction Types, and Spending Limits.

Things to note:
• Existing Debit Card limits set by Citizens Bank Minnesota remain in place. In Card Management you now have the capability to set and adjust additional transaction and monthly limits as desired to further protect your Debit Card from potential fraud. Changes made within Card Management take effect immediately.
• International settings are only applicable if you have contacted the bank for a temporary unblock of international location, for purchase or travel.

WooHoo! Banking®

Citizens BANK MINNESOTA
Member FDIC

WooHoo! IT'S WHAT WE DO!