The Basics of Credit Card Security

How Cards Become Compromised

Data Breaches

When a major financial or retail institution is hacked, that puts your card info at risk (even if you haven't made a recent purchase.)

Payment Card Skimming

If attached to a card reader, a skimmer device will capture and store your card info. Common at gas stations and ATMs.

Public Wi-Fi

Hackers get easier access to your data over an unsecured connection.

Phishing Attacks

A fake email, text or call that may look legitimate but ultimately try to alarm or scare you into providing personal information.

Installing Malware

Malware can be downloaded unknowingly through an email attachment or fake software update. Hackers can see all your computer activity, including any sensitive information you enter.

Protecting Your Personal Data

- Enable notifications anytime a purchase is made on your card.
- Contact your bank right away if you see an unfamiliar charge, even if it was just 50 cents (that's typically how thieves test the stolen card.)
- Consider services like LifeLock that alert and assist you whenever there's a threat to your identity online.
- Create unique passwords that are at least 12 characters long with a combination of letters, numbers and symbols — especially for sites that require payment info.

Things to Avoid

- Saving full card numbers in your web browser.
- Storing security codes.
- Exchanging card information via unencrypted email.
- Sharing card numbers over the phone, especially if the service called you.
- Keeping written card information in plain sight.

SOURCE: Federal Trade Commission, The Balance