Tips for Avoiding Credit Card Fraud

With nearly 38,000 complaints logged in 2015, credit card fraud ranks as the second most common form of identity theft, behind only tax- or wage-related fraud, according to the Federal Trade Commission.

It can take many forms, including:

- Scammers who try to sucker you into giving up credit card info over the phone.
- E-mail phishing.
- Skimmers – devices hidden in the mouths of card slots at gas pumps, ATMs and even restaurants to copy card information.

Nothing but healthy skepticism can save you from falling for a slick hustler. But advances in technology are designed to better protect consumers against credit card fraud when making purchases in person.

EMV cards

Though they've been used widely for years overseas, EMV cards are relatively new in the U.S. They still have the thick black band on the back, so they can continue to act like the “magstripe” cards that people have been carrying in their wallets and purses for decades. The brainy component is the chip embedded in the card, indicated by a gold- or silver-colored foil square on the front.

When inserted into an EMV reader, the chip generates a unique, encrypted transaction code, or token. When the token reaches your bank, it is decrypted to verify your account and authorize the payment. Since the token changes with every transaction, a stolen token can't be reused.

By comparison, the information on a magstripe is unchanging, meaning it's easily cloned. In the U.K., where EMV has been in use more than a decade, the switch cut in-person credit card fraud by more than two-thirds.

Bear in mind that EMV chips are no safer than magstripes when you're buying online or giving credit card info to someone over the phone. And for now, most gas pump card readers aren't EMV-ready.

Mobile payment services

“Mobile wallets” or “e-wallets” use the same kind of token technology as EMV cards. The difference is that instead of pulling out your card, you tap or scan your smartphone at retail checkout terminals.

Depending on the smartphone pay system, you may need to enter a PIN or scan your fingerprint to complete a transaction. With Apple Pay, Android Pay and Samsung Pay, you're assigned a substitute card number that's unique to the phone and tethered to your credit card number.

Using your smartphone or tablet adds another layer of security, because a hacker would need to have both the device and its password.

Monitor your credit card statements

It's a good idea to check your accounts regularly. If you see charges you know you didn't make or otherwise don't recognize, contact the card issuer to clarify and, if necessary, dispute them. You may also want to set up a fraud alert or request a credit freeze.

Online transactions

If you're buying online, make sure you're on a secure site before you enter sensitive information. Look for the *https://* or a padlock at the start of the web address.

It's also wise to avoid accessing bank or personal finance sites using public Wi-Fi, which can are wide open to hackers.