For most of us, swiping or inserting a debit or credit card has become second nature. We do it at gas pumps, ATMs, and retail checkouts without a second thought. Unfortunately, thieves are counting on that convenience. Card skimmers, tiny, hidden devices criminals install to steal card data have been on the rise for years. Despite increased awareness, myths about skimmers continue to circulate, leaving consumers with a false sense of security.

Let's cut through the noise and separate fact from fiction.

Myth #1: You can spot a skimmer just by jiggling the card reader

In some cases, external skimmers that clip onto the front of an ATM or gas pump reader may feel loose, but criminals have gotten much more sophisticated. Many modern skimmers are installed inside the machine, directly on the card reader's circuit board. These "deep insert skimmers" are invisible from the outside and won't budge no matter how much you push or pull.

The jiggle test might occasionally detect a crude overlay, but relying on it is like trying to catch a pickpocket by patting your pockets once in a while, it won't stop most thieves.

Myth #2: Skimmers only target shady or out-of-the-way locations

Skimmers have been found everywhere, from rural gas stations to high-end banks in busy downtown areas. Criminals don't just target "bad neighborhoods." They look for machines with poor security, easy access, or a lot of foot traffic.

In fact, busy locations are often more attractive to criminals because a higher number of cards means more stolen data in less time. Assuming a location is safe simply because it looks clean or upscale can make you more vulnerable.

Myth #3: EMV chip cards can't be skimmed

Chip technology is safer than magnetic stripes, but it's not foolproof. Skimmers can still intercept data from the card's magnetic stripe, which many cards still carry for backward compatibility. Some devices also use shimmers—thin, card-like inserts that sit inside the reader—to capture data from the encrypted chip interface itself.

Worse, criminals often pair skimmers with hidden cameras or fake keypads to steal PINs. Even if the chip prevents duplication of your exact card, thieves may use the stolen data for online fraud, where a physical card isn't required. And to make matters worse, many criminals physically jam the EMV slot with obstructions or even super glue forcing consumers to resort to using the less secure magnetic card swiper on the POS (Point-of-Sale) terminal.

Myth #4: You can always see when a pump or ATM has been tampered with

In the early days of card skimming, clunky overlays and mismatched plastics sometimes gave skimmers away. Today, many devices are custom-made to fit perfectly and look identical to factory equipment. Unless you're trained to spot subtle signs of tampering, you may never notice.

Some criminals don't alter the outside of the machine at all—they open the cabinet with stolen keys or universal pump locks, then install internal skimmers that leave no visual trace. From the outside, the machine looks perfectly normal.

Myth #5: Contactless payments (tap-to-pay) are just as risky

While some people worry about "wireless skimming" or thieves reading cards from a distance, this is far less common than card reader skimming. NFC-based contactless payments use encryption and dynamic transaction codes, which are very difficult to clone. In reality, tapping your card or phone is usually safer than swiping or inserting. However, that hasn't stopped some criminals from drilling directly into the NFC interface, thereby disabling the tap-to-pay option and forcing users to the less secure magnetic card swiper on the POS (Point-of-Sale) terminal.

Myth #6: If you check your bank statements often, you don't need to worry

Monitoring your accounts is important - it helps you catch fraud quickly. But by the time you see unauthorized charges, your information has already been stolen. Early detection is valuable, but prevention is better. Once your data is compromised, you may spend weeks replacing cards, updating accounts, and disputing charges.

The Role of Law Enforcement and Specialized Tools

Because skimmers are harder to detect, law enforcement agencies and fraud task forces have turned to specialized tools that can scan for hidden devices inside payment terminals. These devices are currently in use by local, state and federal law enforcement and have helped prevent over $200 million in fraud in 2025 alone. View more details on this ongoing anti-skimmer operation.

For the average consumer, the best defense is awareness, vigilance, and choosing safer payment methods like tap-to-pay or mobile wallets. But the real fight against card skimming is happening behind the scenes, where trained investigators and specialized detection equipment are the only sure way to uncover the devices we can't see.