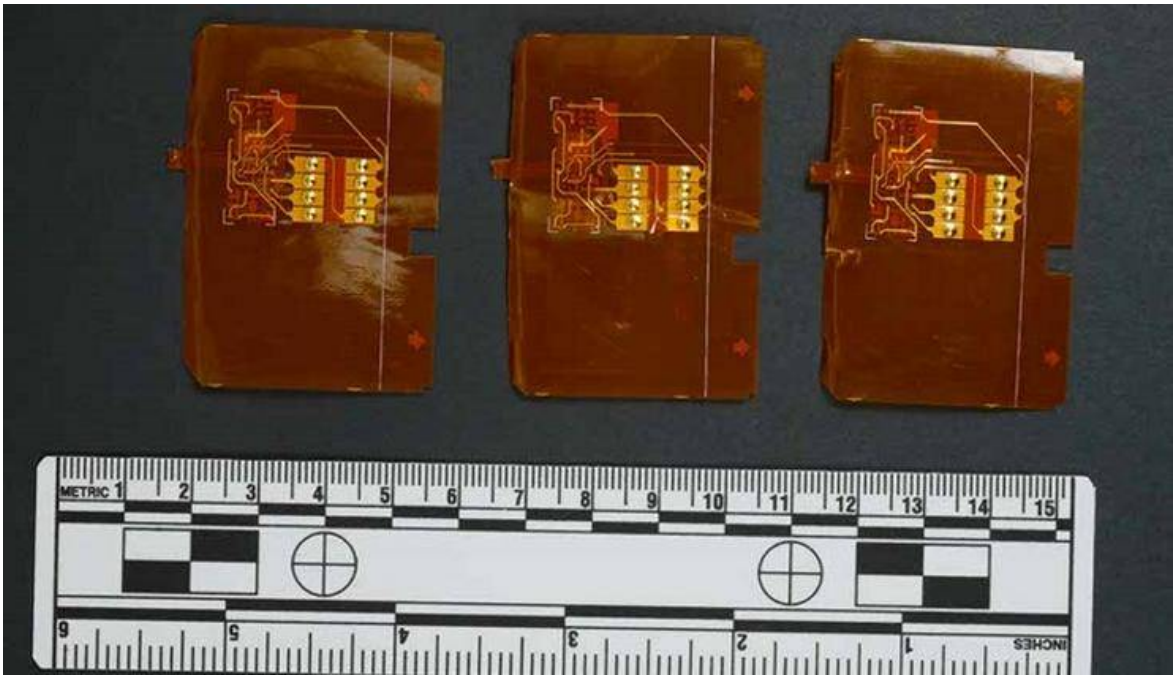

Shimmers: Latest Threat To Credit Card Security Is Undetectable

Technocrats that build technology for mass consumer applications apparently have blinders on when concerns security. They think that they are going to save mankind, but they are easily outwitted by creative hackers. TN Editor

When using an ATM to withdraw cash or to check available funds, there's a number of things you can do to ensure safe access to your account. These include covering the keypad when entering your PIN, checking no one suspicious is standing nearby, and looking the ATM over to see if it has been tampered with. However, none of those steps can help you avoid the latest threat to your card's security: shimmers.

You've probably heard of a skimmer before. Skimmers are used to swipe and read the magnetic strip on a card and criminals have found novel ways to add them to ATMs. For example, they construct a new front for an ATM and stick it over the top of the real one. Some even integrate a camera to try and record your PIN (which is why you should always

cover your hand when typing it in).

Skimmers work, but are bulky and relatively easy to spot. Shimmers are different. They take the form of a very thin card with an embedded microchip and flash storage which is slotted inside the card reader. You cannot tell the shimmer is inserted, and it doesn't stop cards from being used in the machine as normal.

When someone uses the ATM their card details are recorded by the shimmer. Criminals will obviously prefer using a shimmer because it's very easy to install without being detected. It gets worse, though, as reading the data the shimmer stores can be done simply by inserting a special card. So the criminal can collect the stolen data while looking like they are simply using the ATM to access their account.

Because these shimmers are so thin and card sized, they aren't limited to just ATMs. The terminals we increasingly see installed in stores for self-service are also vulnerable.

Read full story here…