The Anatomy of a Card

Magnetic Strip

The magnetic strip on the back of a debit or credit card holds several key pieces of information about the card, including the card number and expiration date.

Someone wishing to steal this information can only do so by physically swiping the magnetic strip. Thieves usually achieve this by attaching a "skimmer" to an ATM machine or POS terminal. When you swipe your card to retrieve cash or pay for a transaction, the skimmer collects the information from the strip, and you are none-the-wiser.

Before you use your card, pay close attention to the machine. If there appears to be anything attached, or it appears to have been tampered with in any way, don't insert or swipe your card, and notify the owner of the machine immediately.

Card sleeves will protect the magnetic strip from being damaged, but are not designed to protect information from being stolen.

RFID

Some debit and credit cards have an RFID chip inside of them (though most do not) and are usually identified by a symbol printed on the card, such as the one pictured here. *NOTE: Georgia Power Northwest credit and debit cards DO NOT have RFID chips.*

RFID chips are supposed to make using your card more convenient. Rather than swiping a card, all you have to do is place it near the point-of-sale device, or "tap" it on the device, and your card information is transmitted to the machine. However, someone wishing to steal this information can easily do so with a device of their own, and they never have to touch the card to do it. They can actually brush up against your purse or wallet, and voila, they have your card information.

There are specially designed RFID-blocking sleeves that will protect your card information while it is secured, but the best defense against this particular type of theft is to NOT have an RFID card at all! The convenience simply isn't worth the risk!

EMV Chip

Finally, there is the EMV chip. This chip, embedded in your card, is the newest technology available for protecting your card information. Rather than "swiping" your card, or "tapping" your card, you must insert it into a machine capable of reading the EMV chip. Unlike magnetic-stripe cards, every time an EMV card is used for payment, the card chip creates a unique transaction code that cannot be used again. If a hacker stole the chip information from one specific point of sale, typical card duplication would never work because the stolen transaction number created in that instance wouldn't be usable again and the card would just get denied.

EMV chips have been in use in Europe for several years, and so far, thieves have not been able to find a way to steal information from chipped cards. Until they do, this is by far the most secure type of card available.

It is important to note, though, that almost every card that has a chip still has a magnetic strip on the back. Many merchants, and most ATM's are still not capable of accepting the chip, so you should still use the same precautions mentioned above when swiping your card.

It is also important that you not allow your card to get bent, as the chip can be delicate, and even a small bend will make it unusable.