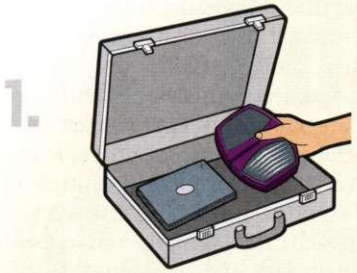
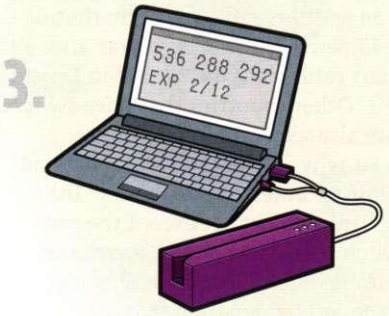
Newer cards can be hijacked, too

Playbook for a crook

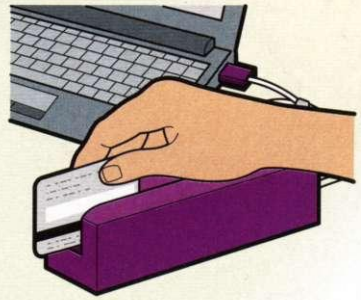


THE SETUP **Thief connects a battery-powered card reader to a netbook in briefcase, which conceals the devices.**

THE SWIPE **Crook carries briefcase close to consumer's purse or pocket, where contactless cards might be carried.**



THE DISPLAY **Card information obtained in step 2 is displayed on a computer attached to a magstripe-writing device.**



THE CLONE **A blank magstripe card is put through the device to make a counterfeit card.**

ILLUSTRATION BY BROWN BIRD DESIGN

A lesson in card cloning

Check your wallet. You might not know it, but you could have a credit or debit card that uses a tiny computer chip and a radio antenna to transmit account information from your card—even when you're not shopping.

MasterCard uses "PayPass" to identify the cards. Chase bank coined the term "Blink." Some contactless cards, which use a radio frequency identification, or RFID, chip, might simply have a symbol on the card consisting of four curved lines (shown at right). An industry newsletter, The Nilson Report, says 35 million contactless chip cards are in circulation in the U.S.

The cards are touted as convenient, but they are also vulnerable to being skimmed without ever leaving your pocket. The information communicated from your card to a card reader can be enough to create a counterfeit card that can be successfully used to make an unauthorized purchase, as we observed in a recent demonstration by Recursion Ventures, a security research and consulting company in New York City.

The basic equipment needed for that form of fraud is readily available to would-be crooks. An electronic card reader available online for less than $100 can be connected to a laptop to store skimmed information. When Chris Paget, whose title at Recursion is chief

hacker, used such a reader to scan a Chase debit card he'd recently received, the card's account number, expiration date, and security data immediately appeared on the computer screen. Two credit cards still inside the mailing envelope revealed the same type of account data.

Making a counterfeit. From a few inches away, the account data can be read even if the card is inside a wallet or purse. By transferring the skimmed card data onto a blank magnetic-stripe card, Paget produced a counterfeit card that he then used to make a purchase that was successfully processed.

Chase spokesman Paul Hartwick says the security codes on its contactless cards are designed to change with every transaction, as they are with most RFID-enabled cards, so that even if a card is counterfeited, it would work for only one fraudulent transaction.

"If I put a reader next to a turnstile at Grand Central Terminal at rush hour, I could probably capture data from 5,000 cards in an evening, and what you're getting from each one is enough to initiate a transaction," says Mark Rasch, a former Justice Department computer-crime prosecutor who serves as director of cybersecurity and privacy consulting at CSC, a business technology firm. Moreover, repeatedly scanning a card that is lost, stolen, or intercepted in the mail produces multiple security codes, Paget says.

The Smart Card Alliance, an industry group, maintains that contactless card technology deployed by American Express, Discover, MasterCard, and Visa is secure and that there have been no reports of consumers being victimized. American Express says its contactless cards do not reveal the card account number, and that was the case in the demonstration we observed.

Mixed results for shields. The absence of a flood of fraud reports linked to the cards is not proof of their security, though, according to Kevin Fu, a University of Massachusetts at Amherst assistant professor who has published research on the topic. Because the contactless cards in circulation in the U.S. represent only 3.5 percent of the total debit and credit cards in use, they have not yet presented a big enough target to lure many crooks, especially when traditional magnetic stripe cards are so easily counterfeited.

Shields or wallets marketed as RFID-blocking devices can make it more difficult for someone with an electronic reader to read your cards, but they don't entirely block transmission of card data. When Recursion's security experts tested 10 types of shields and wallets currently being sold to protect contactless cards, they found that none blocked the signal completely, and there was dramatic variability even among samples of the same brand. Using a different approach, Recursion's experts created a credit-card-sized jamming device for the wallet that prevents cards from responding to any reader.

Our reporter offered her own homemade shield constructed of duct tape and lined with aluminium foil. It provided better protection than eight of the 10 commercial products, including a stainless-steel "RFID blocking" wallet selling online for about $60.

Bottom line. Until contactless-card security is improved or better protective devices are widely available, consumers can ask for cards that are not RFID-enabled, a request that at least some major card issuers say they will honor.

FOILED AGAIN **A duct-tape wallet lined with aluminum foil made RFID cards more difficult to read.**