



## World Vision Security

### How do credit card numbers get stolen?

When you use your credit card to make a purchase, the card number is sent through a payment network. If a hacker can gain access to any part of this payment network they can steal your credit card information.

The payment network begins at the point where you enter your credit card information. This can be a swipe terminal in a store or restaurant, an online shopping site, or on a paper form like a magazine subscription, a utility bill, or a tax form. Paper forms are the easiest to compromise because the form contains the full credit card number. By contrast, electronic entry (swiping) is difficult to compromise because only the last four numbers of the card are visible. Hackers steal credit card numbers online two different ways. The hacker may have compromised an online shopping site you visit, or they may compromise your PC with a malicious program that steals your credit card and bank account information.

### How do hackers do this?

The most common way is **Phishing**. Phishing is an attack that uses cleverly designed emails to get you to give your credit card information directly to the hacker. The email is a fraud but it looks like it is from someone you actually do business with such as your bank, a store or an auction site. **Framing/Poisoning** is probably the second most common attack. The hacker replaces the real pages on a web site with pages that send you to their site where they steal your credit card information as you enter it. A poisoned web site can download and install a program to capture what you type on your keyboard: passwords, credit card numbers and bank account information. The Hannaford Brothers grocery chain hack is an example of a **Merchant/Processor Breach**. Hackers installed a program on check-out systems that stole customer debit card numbers and pins. **Skimming** uses a device mounted to a card reader (e.g., on a gas pump) that captures the credit card information when the card is swiped.

### How can I protect myself?

There is very little you can do to protect yourself against Skimming and Merchant/Processor attacks but here's what World Vision Information Security recommends to our employees to protect against Phishing and Framing/Poisoning attacks:

1. **Install anti-virus** on your computer and keep it up-to-date with the latest virus signatures. Do a full virus scan of your computer at least once a week. If your computer has firewall software, turn it on too!
2. **Never use your debit card** for Internet or paper/form-based transactions. Get a low limit (e.g., \$1,500) credit card you can use exclusively for these types of transactions.
3. **Never follow links or open attachments in emails** unless you are absolutely sure who sent this email to you.
4. **Never follow links or take any actions on things that happen on your system randomly** such as pop-ups that say you have 30 viruses on your system and need to clean them right away! Unless you are absolutely sure the action is safe (for example, an update from Microsoft), **DO NOT** click on anything! Just close the message window by clicking the red X in the upper right corner. If you cannot exit the program then the best thing to do is restart your computer.

#### Very Important Note

If you've already been a victim of credit card or banking fraud, you may have a virus or other harmful programs running on your computer right now that are stealing your credit card, bank and other personal information! Be safe; get your system checked out by a PC professional as soon as possible.