Credit card security

Your Your Full Number MA07A00 A0128S18 Credit Card Security

CyberSource has recently reported that 40 percent of Britonsavoid shopping online due to issues on security of personal information. Study shows that more than one-third of poll respondents know of someone being defrauded online. Furthermore, 70 percent of the respondents have credit card safety subscription programs that are designed and promoted by big credit card companies like Visa, American Express, and MasterCard. Visiting the American Express website, it is clear that the company has designed a measure to protect their credit card holders; this is known as the Fraud Protection Guarantee, wherein the card holder is free from any fraudulent charges whether the credit card is used on the internet or not. It promotes maximum security because of its secure encryption technology that keeps the cardholders information strictly confidential (americanexpress. com, n. p.). For secure and safe online shopping, MasterCard has its MasterCard Secure Code; it works as having a personal code only known to the cardholder. Visa on the other hand, is also cooking up its own scheme of credit card security measure.

Credit card use pose dangers as credit card fraud today do not only happen when a credit card is stolen. Aside from stolen credit cards that make up 23 percent of card frauds, there is the

Your Last Name 2

counterfeit credit card, which makes up 37 percent of credit card frauds. Criminals who make fake credit cards employ the latest technology to " skim information" that are embedded on the magnetic stripes of the credit card and pass security measures, like holograms (" Credit Card Fraud Statistics and Facts," n. p.). In other words, using credit card online makes you

susceptible to all kinds of credit card fraud.

One interesting question is how criminals get a hold of your information. Although the most common perception is that credit card info is intercepted once the card is used online. That is an interesting theory, but experts explain that e-commerce has created an environment where anonymity is practiced; meaning cards are being used even without identifiers (Faughnan, n. p.). This could be the one problem that big credit card companies try to address with the code systems of their new security measure program. Another way of stealing a cardholders information is using a particular online business as a front to get credit card info. One common and enticing site is pornography site. Such is designed as a legitimate business, thus can easily asked for a persons credit card information once that person is interested in one of the sites services. This is what is identified as selling information because these are vendors and purchasers that only deal with information and need no physical address for the business (Faughnan, n. p.). Networked transactions is one of the identified way how personal information is gathered through the use of credit card in online purchases. This type of transaction is said to enable criminals " to test credit card numbers across the Merchant Account System in high volume, and due the large volume of credit card numbers involved, detection is delayed and making prosecution difficult as well.

Bibliography

" Fraud Protection Guarantee." americanexpress. com. 30 April 2009.

.

" MasterCard Secure Code." mastercard. com. 30 April 2009.

.

" Credit Card Fraud Statistics and Facts." spamlaws. com. Royal Canadian Mountain Police. 30

April 2009. .

Faughnan, John G. " E-Commerce: Connection and Implications." 30 April 2009.

.