SAVVY AND SAFE

Most people know how to stay safe in the city: Don't walk alone after dark, hold onto your bag on crowded subways, and only ride in registered cabs. However, many people are not so savvy when it comes to staying safe on the Internet and don't know what to look for. Identity theft – when thieves steal your personal information and use your identity to open bank or credit card accounts or take out home loans in your name – is on the rise. In some cases, thieves charge thousands of dollars to credit cards, empty bank accounts, and can ruin your credit. Criminals are getting better at cheating you out of your money. What's worse is that they sometimes do it with your help. To avoid becoming a victim of an Internet scam, know what to look for.

DON'T BE THE VICTIM OF A SCAM

The friend in need scam Have you ever received an email from a friend who is overseas and urgently needs you to send money? Emma Park did, and it cost her $2,000. Emma, 22, from Chicago, was the victim of a scam. Somebody hacked into her friend's email account and sent urgent messages to everyone in the contacts list. Emma didn't even think of calling her friend to check if the email really was from him. She sent the money, and by the time she realized it was a scam, it was too late. Emma never got her money back.

DON'T send money to anyone if you get an email like this.
DO contact your friend to ask if there is a problem.

Information-request scam Your bank sends an email saying it has lost customer data. It asks you to send your bank account details, including your full password and PIN[1]. At least the email *looks* as if it's from your bank. It has their logo and looks official.

DON'T reply! Banks and credit card companies *never* ask for your full password or PIN in this way.
DO check the spelling and grammar. If there are mistakes, the email is probably a scam.

The "make money fast" chain email scam Someone sends you an email with a list of names. It asks you to send a small amount of money to the person at the top of the list, delete that name, and add your name to the bottom. The email explains that when your name gets to the top of the list, you'll receive a lot of money. You might even become a millionaire! Usually, however, the scammer's name stays at the top of the list, so he or she gets all the money.

DON'T forward the email. Sending this type of chain email is not only expensive, but it's also illegal.
DO block the sender, and block any emails that come from names you don't recognize.

Being savvy about scams is the best way to stay safe. If something seems a little strange, it probably is. Don't fall for it.

1. *PIN*: Personal Identification Number

C Are these sentences true or false according to the article? Write *T* or *F*.

1. Most people know how to recognize scams on the Internet. ____
2. Identity theft is increasing. ____
3. Emma lost $2,000 of her own money. ____
4. Emma sent money to a friend who was traveling overseas. ____
5. Your bank may ask you for your password if they lose it. ____
6. Your name will never get to the top of the list in the chain email. ____