REGIONS

Tips for Preventing Credit Card Fraud

The cost to card issuers, retailers and consumers of U.S. debit and credit card fraud grew by 29 percent to $7.1 billion in 2013, according to data from Business Insider (BI) Intelligence.

Yet, with a little care and savvy, you can reduce your vulnerability. Here are six tips to help you safeguard your accounts.

1. Carry Only the Credit Cards You Need

You may have several credit accounts, but that doesn't mean you need to carry cards for each one. Carry only the cards you need each day to minimize the damage you could experience in the event of credit or debit card theft. Keep the cards that you don't carry in a safe and secure place.

2. Protect Your Personal Information Online and Offline

Credit card fraudsters often collect personal information such as birthdates, addresses, passwords, and account numbers, then use the combined information to impersonate their victims. So think twice about sharing your personal information on social networks.

Computer hacking techniques are always evolving, so make sure your smartphone, tablet, and computer are password-protected. When you create your password, always use a mix of letters, symbols, and numbers rather than a simple word or date, and don't use the same password for every device or account. If you want help creating a strong password, you can use password-protection programs such as Dashlane or LastPass. It's also a good idea to avoid entering important passwords, such as the login to your bank account, on public Wi-Fi networks. If you need to use public Wi-Fi networks often, consider subscribing to a virtual private network (VPN) service that provides internet browsing protection.

Offline, don't put sensitive records in the trash or recycling bin. "People throw away the darnedest things," says identity theft expert Wayne Black, president and owner of Miami-based investigative firm Wayne Black & Associates. Thieves sift through garbage to find information they can use, so Black suggests shredding sensitive documents like a draft tax return or mortgage application before you dispose of them.

3. Review the Vendors and Amounts that Appear on Your Credit Card Statements

Black says one of the most frequent and insidious credit card scams involves a legitimate purchase with an inflated total charge — a doctored tip amount at a restaurant, for example, or a fake "cash back" amount added to a gas station purchase. He recommends keeping receipts from gas stations and restaurants, then comparing them to the totals on your statement. Also watch for phantom charges from vendors you don't recognize, and always report suspicious activity right away.

4. Check Your Credit Report Every Four Months

Fraudsters who have collected your personal information may try to open new credit accounts in your name. By regularly monitoring your credit report, you can identify and address credit card fraud quickly. You can access your credit report for free once a year from each of the three major U.S. credit bureaus — Equifax, Experian, and TransUnion — through annualcreditreport.com. By staggering your requests, you can check a credit report every four months. (For example, you might request your credit report from Experian each year on Feb. 1, from TransUnion on June 1, and from Equifax on Oct. 1.)

5. Tell Your Credit Card Company When You Plan to Travel

Before traveling out of state or going abroad, Black calls his credit card providers to tell them where he's going and how long he'll be there. In addition to preventing credit accounts from being frozen because of unusual activity, it lets card issuers know that any activity near the home base during this travel period could be fraudulent.

6. Verify Before You Give Away Credit Card Information

Don't give away your credit card number over the phone unless you're certain that you're dealing with a reputable party. Protect yourself by always initiating calls where you'll need to share personal details. If a caller asks you to confirm personal details on behalf of a company, calling the company back using their official customer service phone number can help you avoid credit card fraud.

The same goes for online transactions. Never give out personal information to strangers who contact you via email. If they say they are from a company you do business with, go to its website and reply directly to the customer service team. If you click a link that is supposed to navigate you to a new webpage, verify that the new URL matches that of the company you're attempting to pay. A hacker's site will redirect you to a URL that you may not recognize, so avoid entering personal information on websites that have strange URLs.

By following these six tips, you can reduce your risk of becoming the victim of credit card scams.

This article can be found at regions.com/advice/preventing_credit_card_fraud.rf

Online & Mobile Banking Security:

How to protect yourself:

- **Protect your Online ID and Password.** Never share your Online ID or Password with anyone. Do not save your Password in your browser.
- **Never share your Security Questions and Answers.** If our system detects an unusual pattern with your login, you will be prompted with one of these questions. You must answer correctly before logging in; helping to prevent unauthorized individuals from accessing your account.
- **Keep anti-virus software up to date and install regular system updates.** This will help protect your computer from receiving viruses; leaving your information vulnerable to compromise. Read more on this topic.
- **Review your account statements every month.** If you find a transaction that you did not authorize, you must tell us within 60 days of the date that your statement was delivered.
- **Call immediately**. If you believe that your Online ID and Password has been lost or stolen, call us at 1-800-734-4667. Also, if you receive an email asking you to provide your Regions Online ID, Password, Social Security or any other personal information, please contact us immediately. **We will never ask for your personal information through an email.** We also ask that you forward the suspicious email to phishing@regions.com.

This information can be found at regions.com/personal_banking/online_security.rf