**Credit Card Fraud: Tips to Avoid it this Christmas**

With Christmas right around the corner, credit card shopping will take a boost - and so will the attempts of cyber criminals to get access to cardholder data. Though there is no way to ensure that you will not be a credit card fraud victim, there certainly are ways you can adopt to minimize your risk. Let’s look at some tips on how you can avoid credit card fraud this Christmas.

1. **Don’t buy from unfamiliar websites**

We all love online shopping, but one has to be very careful when entering their credit card information on a website. Always buy from trustworthy sources and avoid conducting transactions on unfamiliar websites. Do not buy if a website does not offer a safe payment gateway like PayPal.

Furthermore, be wary of risks that can potentially arise as a result of using online payment services that need your credit card details. If the service gets hacked or has its website accessed by a malicious user, it can also put your personal data at stake. To prevent this, verify that the website should have a lock sign shown in the browser and have an address starting with “https” instead of http, which means that the website is using a secure protocol.

1. **Regularly check your credit history**

Keep track of your credit history by getting a copy of your credit score. It can alert you about attempts that are made in your name to apply for credit.

1. **Keep your system updated and secure**

Always keep the computer that you use for shopping updated with latest patches and installed with latest antivirus updates. Also keep your mobile devices updated and do not buy through apps that don’t have good rating or have a questionable security.

Never click on unknown links that offer Christmas rewards or points without confirming their authenticity. Same goes for emails. Do not open suspicious emails asking you to open a link or enter your information as they are usually phishing scams that can collect your financial data.

1. **Do not throw your documents in the bin**

If you need to dispose off any of your documents that have your personal details on them, do not throw them directly in the bin. Instead, use a shredder or make sure you make them illegible before throwing them away.

1. **Never give credit card credentials over the phone**

Always give your details through a secure payment method and never tell your personal information to anyone over the phone. A scammer can impersonate as someone else and get your personal data.

1. **Use a Secure Network when Shopping online**

When conducting an online transaction, never use a public WiFi. If your network is not secure, all your personal information stored on your connected device or sent over the internet such as card numbers, social security number, bank details and more can be accessed by hackers easily. Always use your personal password protected WiFi for online shopping. If you don’t have that option, consider installing a Virtual Private Network (VPN) which directs your browsing over a secure and private network.

Also remember to keep strong passwords for your personal devices such as laptops and phones.

1. **Always Keep your Card Safe with You**

The [card manufacturing process](http://www.cardzgroup.com/BankCards.html) keeps on evolving - and with the new contactless Near Field Communication (NFC) technology like PayPass, PayWave and Tap & Go – it’s very easy for hackers to access your card and conduct transactions through it if they are in close proximity with you. Hence, it is important that you keep your card secure with you inside a thick layer of wallet or a card protecting device so that people near you cannot access your information.

1. **Be vigilant when opening a new retail credit account**

Nowadays many stores provide incentives and discount offers for people who open store credit card accounts. It’s very important to be careful and pay attention during the entire process of enrollment. For instance, when opening the account, you may be asked to enter your Social Security number or date of birth. When doing so, make sure that no one is spying over you and tell the sales personnel that you are concerned about how this information will be disposed off after it gets entered into the system.

1. **Be wary of Skimming devices**

A skimming device can copy your card data. When using a card reader or withdrawing money from an ATM, make sure that there is no skimming device attached to it. Always cover the number pad of ATM machine with your hand when entering your PIN code so that if a skimmer has installed a secret camera to spy on your code, they are unable to see it.

1. **Report your lost or stolen card immediately**

If your card gets lost or stolen, report it to the credit card provider immediately to prevent yourself from further loss. The sooner they get to know, the sooner they will freeze your account. You may deem it unnecessary as it’s possible that you may find it soon after, but the inconvenience of having to wait for the arrival of new card is much more than that of dealing with identity theft and fraudulent charges against you. In order to make reporting fast and simple, save the credit card provider’s number with you.

**Conclusion**

The best way to protect yourself while you make purchases this holiday season is to be vigilant. Don’t trust something if it seems too good to be true. At the same time, don’t let this fraud threat stop you from enjoying this time. Act smart, do your best to keep your personal information safe, and have a Merry Christmas!