**Online Payment Security: 8 Steps to Ensure Safety Transactions**

Online shopping has become increasingly popular in the past few years. But as more people go online to conveniently shop from home, it gives cybercriminals all the more advantage to attack them and use their information to their advantage. This is why ecommerce companies work hard to secure their transactions and build their customer’s trust as the looming threats of cybercrimes can give a reasonable blow to their marketing efforts. Scammers are now targeting both merchants and customers. Once they gain your financial information, they may use it to buy goods and services for themselves, or sell your information to someone else and make a profit.

So what can you do to ensure safe online transactions? The answer: stay aware and take safety precautions. If you want to get the best out of your online shopping experience – without being a target of internet scams and cyber criminals – you need to take some safety steps.

Here are eight security steps that can help you ensure the safety of your online transactions and payments.

1. **Opt for Credit over Debit**

When doing online shopping it is always safe to pay from a credit card instead of debit card. Using a debit card for online payments is risky because it is directly linked to your bank account. If someone hacks your information, they can misuse your debit card to withdraw funds from your bank.

Credit cards are safer and pose lesser liability in case a card number is stolen. Since they have spending limits on them, they can’t be misused the way debit cards can be. Its much easier to dispute fraud charges on credit cards while recovering lost money through debit cards can be a tiring and lengthy process.

One-time disposable credit cards are also used nowadays and are especially designed for online shopping.

1. **Shop from Reputable and Secure Websites Only**

Before you set out to give your personal and financial information, always make sure that you are buying from a reputable and secure website. If the website seems new or unknown, do not shop from there. Hackers can sometimes trick you by creating apparently legitimate ecommerce websites and maliciously retrieve your information to their advantage.

Sometimes a website may be legitimate but not secure. Always buy from a website that says “https” at the beginning of its site address, and not just “http”. The missing “s” in the sites address indicates that it is not encrypted and any data you enter is not secure.

1. **Outsmart Phishing Emails**

One of the oldest yet effective scams of hackers is phishing emails. Holiday season is mostly the perfect time for them to send phishing links promising gifts or special offers. They may also try to get your information by sending you an email asking you to confirm your account information or a purchase. Reputable businesses do not send such kind of emails from unfamiliar accounts. Never click on such links and never provide your sensitive information in reply to an email. If you receive an email from a company or a bank, it is always best practice to type the website address yourself to check the offer or make a call to confirm instead of providing your information.

1. **Beef Up Your Password and Never Save It**

When keeping your private information safe, unique and difficult passwords are always your best gatekeepers. Do not use common passwords or the ones which are easy to guess. Always use a combination of special characters and alphanumeric numbers and keep the password length longer than 6 digits. Never use the same password for multiple websites and never save your password when logging in.

1. **Use Firewalls and Anti Malware**

To protect your digital devices from all classified and unclassified attacks, always use well established [security application](http://www.cardzgroup.com/ContactSmartCard.html) software such as anti-malware software and firewalls. Always keep them updated so that the anti- malware can detect all the newly emerging malware threats even before it makes its way to the automatic updates database.

1. **Don’t Use Public Wifi**

Public WiFi can be like a complementary dessert you get for free. But hackers love them more than you. Networks open to public are not secure, and information entered using a public hotspot is very vulnerable. Cybercriminals can catch your passwords and financial information by intercepting your data, which is why you should never log into payment sites like Paypal or local banks on a public WiFi, and ensure that you log out of such websites on mobiles before you connect to a public network.

1. **Keep Record of your Transaction Statements**

Always keep a check on your credit card transaction statements. Also keep all your purchase receipts and compare them with your transactions statements to ensure that they are accurate. Report immediately if you find any inconsistency.

1. **Be Careful with Shopping Apps**

Mobile apps have made everything convenient for us, including stealing of private information. Always download well-known shopping apps from official stores like the PlayStore or AppStore. Before confirmation, read what permissions the app is asking for. If you see the app asking you access for something beyond its functionality, such as messages, do not allow it to access it. Also check the comments section of an app to see previous buyer reviews before downloading it.

**Final Thoughts**

With all the convenience it provides, online shopping can turn out disastrous if you shop carelessly without taking appropriate safety measures. It is always best to educate yourself and follow best practices of online payments. If you suspect that your payment card or information is misused, inform your bank immediately.