Safety Tips for Shopping Online

What you can do to keep your financial data safe

Shopping online is convenient, fun and growing in popularity, but many online shoppers worry about the impact of data breaches.

Shopping online is convenient, fun and growing in popularity, but many online shoppers worry about the impact of data breaches.

One tip for shopping online with an added layer of protection is to open a credit or debit card specifically for online shopping. If you use a debit card or a prepaid credit card, you can control exactly how much money is at risk. Keeping a separate credit card for online shopping with a low credit limit provides the same type of control and also limits the number of charges on each statement, so you can easily go through the statement and identify anything that seems amiss.

"Also, look into virtual credit cards if your card issuer offers this service," advises about.com Security Expert Andy O'Donnell. "Some card issuers will give you a one-time-use virtual card number that you can use for a single transaction if you are concerned about the security of a particular merchant."

Even if you don't use a separate card for online shopping, examining your monthly credit and debit card statements is very important if you want to keep your data safe. It isn't enough to simply check your balance and scan your statement for big purchases.

"Scrutinize your statement for charges you don't recognize," according to science and technology writer Davey Alba, writing in a 2013 Popular Mechanics article. "These don't have to be massive charges, either. Hackers will often test the waters with micropayments first, amounting to a few dollars or even a few cents. Then, when it seems like the coast is clear, they'll go for a big-ticket purchase."

You can also gain peace of mind by talking to your financial institution or credit card provider to learn what data breach policies are in place. Credit card companies typically offer fraud-monitoring services for free and won't hold you liable for fraudulent charges.

"Some ID-theft-monitoring services are paid, which you can consider, but … your own provider will typically offer one for free, and [that] can be just as dependable," states Alba.

Depending on your provider, you may even be able to customize the specific fraud alerts that are most useful to you and reflect your typical spending activities. Popular options include the ability to receive email, text or phone notifications if a single charge is greater than a certain dollar amount, if daily or weekly expenditures exceed a specified total, or if more than a certain number of transactions occur in a set time period, such as one day. You may also have the ability to receive alerts if spending is in excess of a certain amount you specify or is higher than your past average in a select category, such as merchandise or travel.

"When using the online checkout process of a seller, always make sure that the web address has 'https' instead of 'http,'" states O'Donnell. "Https ensures that you are using an encrypted communications path to transmit your credit card information to the seller. This helps to ensure against eavesdropping on your transaction."

Lastly, make sure to use strong passwords for any accounts you set up with online merchants or financial institutions, and change them frequently. Furthermore, don't enter your payment information if you are not using your own internet service, and make sure that nobody can use your device without a password. If you do end up making a transaction on a shared computer, log out of the store website and clear the browser's cache, cookies and web history.

If you keep these tips in mind when shopping online and talk to your financial institution about data breach policies and fraud alerts, you can gain peace of mind and stay safer on all your future online shopping sprees.