10 Golden Rules For Safe Online Shopping

 Ah, the convenience of online shopping; there's nothing like browsing through the virtual shelves of your favourite online retailer… sitting on the couch, in the comfort of your PJs!

But what can be convenient for some, can also be quite daunting for others. This is because online shopping comes with risks, which can include:

- **Credit card fraud** – as a result of making payments over unsecured webpages
- **Phony online stores** – including illegitimate sites and fake email offers
- **Misleading item descriptions** – when received items don't match their online descriptions
- **Intrusive tracking of web activities** – via "zombie cookies" to deliver advertising within your browser

While it is important to be aware of these risks, they certainly shouldn't deter you from the activity of online shopping all together. As long as you follow our **10 golden rules for safe online shopping**, you should be right as rain. Here are our tips:

Rule #10: Do your research

Only ever purchase from **reputable online shopping sites**. Do some digging first to verify the legitimacy of any online store you're planning to transact with. You can do this by searching for consumer reviews about the site and its products and by also looking for a physical address and contact phone number for the company.

Rule #9: Be suspicious of unsolicited emails

Scammers rely on people responding to emails that offer fake bargains. If you receive an email from a company you don't recall subscribing to, **simply delete it**. It's not worth the risk, as these kinds of emails are likely to include links that direct through to malicious sites.

Also, never supply your credit card details to a company via return email. Opt for an alternative way of processing payment for better security.

Rule #8: Don’t be click-happy!

Don’t just click on any old enticing link you see within an email, ad, tweet or Facebook post – unless you are 100% sure it’s legitimate. **Offers that seem too good to be true usually are**, and cybercriminals use them as bait to tempt you in to clicking malicious links.

The best thing to do is roll over links with your mouse, or hold your finger on the link if using a mobile device. This will enable you to see the web address they’re leading to before choosing to proceed.

Rule #7: Look for signs of security

If you’re going to submit personal details to an online retailer, it’s crucial that you know what a secure website looks like. Always look for:

- A **padlock symbol** in the address bar of your browser
- **“https://”** in the web address – the “s” indicates a secure connection
- The address bar or name of the site owner should be **green in colour**

Don’t enter enter any information on a website that doesn’t include these.

Also take care should you be redirected to a third-party payment system. Be sure to run through these checks again if this happens.

Rule #6: Beware of free public WiFi

Using free wireless networks to do your online shopping (as well as internet banking) may be a cost saver at the time, but might also cost you a whole lot more down the track! **Think carefully about using any unsecured network to perform important transactions**

Rule #5: Separate your passwords

Some online shopping sites may ask you to create an account with them, so that when you return at another time, you don’t have to enter your information again. Although this may save time, if you’re unsure whether you’ll actually return to the site again, we’d advise skipping this option.

If there is no choice and you have to provide a password for your account with the online retailer, **ensure you use a password that’s new and unique**. It should be a password that has never been used anywhere else for maximum security.

Rule #4: Double-check all purchase details

Before confirming any payment, be sure to look over all the details of purchase, including:

- Postage and handling costs
- When payment is required (before or after the item arrives)
- When the item will be shipped
- Whether the item is trackable during postage

- How the product is returned should there be any problems (and who bears the cost of this)

When transacting with an international site, check **the currency you'll be paying in**, what the exchange rate is and if any sales duties or taxes will be imposed on your purchase when it gets to you.

It's also important to **know exactly what you're buying and what the dimensions are**. It's not ideal to end up with an item that is either a lot smaller or a lot bigger than what you thought. It pays to carefully read the fine print and not solely trust any product images, as they can be deceiving.

Finally, **take care when entering your information during purchase**. Make sure the number of units, item code(s) and your postal address details are all correct. Always review the information before confirming the order.

Rule #3: Keep a paper trail

Although online shopping often leads to a paperless transaction, this doesn't mean that you shouldn't **keep records of your purchases**.

Don't rely on receiving an email receipt from the site you've purchased from. In fact, it's good practice to print out a hard copy (or take a screen shot) of the "thank you" or "order confirmation" page when you get to it. This will provide evidence of your transaction, including the web address, which may come in handy later on as a form of proof of purchase.

After purchase, **check your bank statement carefully** to make sure the correct amount was debited.

Rule #2: Do use a credit card (it's safer than what you think)

Many people will be surprised to hear that **paying by credit card can actually offer greater protection than most other payment methods**. This is because they don't directly remove funds from your own bank account, so if a fraudulent transaction takes place, the card holder may never end up out-of-pocket. They'd simply need to contact their card issuer to arrange a chargeback (a payment reversal). Credit card issuers and banks are often very helpful in these kinds of situations.

It's also wise to consider using a **separate credit card just for online shopping**. This will limit your exposure and make tracking your purchases a lot easier.

If you don't use a credit card, **PayPal is another secure method of payment** you can use.

Be wary of sites that insist on the transfer of money via Western Union or direct bank deposit. This is often a sure sign they're not legitimate, and therefore a recipe for disaster!

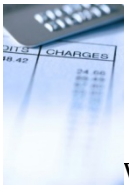
Rule #1: Secure your PC and mobile devices

The ultimate safety of your online shopping experience begins with the computer or mobile device you're using to purchase with. Ensure you have the latest updates installed and that you're using an up-to-date antivirus, or better yet, a full internet security suite, to protect yourself.

At Kingsway Computers we use and recommend Bullguard Internet Security.

By following these 10 tips, you'll find yourself with increased confidence and safety in online shopping world.

Protecting Your Money From Cybercriminals – Some Easy Tips



We've all heard the horror story: someone logs into their internet banking, checks their balance at an ATM or goes to use their credit card – and realises that their bank account has been cleared.

As much as we all fear this happening to us, the truth is, it's not the only example of financial cybercrime. Some hackers won't empty bank accounts straight away, but rather **organise small transactions here and there – adding up to a lot of stolen money over a long period of time.**

See, we tend to notice when a large amount of money goes missing from our accounts (although thankfully, it's usually shopping that's to blame, not cybercriminals!). But a lot of us aren't quite as vigilant about double-checking small transactions on credit cards and bank accounts. Things like grocery shopping, iTunes or Amazon purchases, phone credit, petrol… we don't always keep an eye on the minor transactions that we make throughout our day.

Cybercriminals can mimic these small transactions, drawing money out of an account bit by bit via transfers or payments. The longer this goes on, the more difficult it can be to prove the theft to when the account holder finally realises what's going on.

Don't get too worried, though. The best way to prevent this kind of cybercrime affecting you is to just **keep an eye on your bank and credit card statements** (you can even do this with online banking – just log in and have a look at the latest transactions on your accounts). Look for anything that doesn't seem quite right, like:

- Doubled-up transactions
- Payments to names or companies you don't recognise
- Activity on days that you know you didn't use your account

If you're keeping an eye on your accounts as well as using an internet security package (which has a firewall and identity protection for secure internet transactions), you'll be well placed to keep your accounts safe and secure.

You should also take comfort in the news that the technology protecting your accounts is improving. We were excited to read about Continuous Transaction Monitoring (CTM), a new analysis tool that is helping financial institutions find and stop suspicious account activity in real-time (this is the sort of reason that your bank sometimes knows about your account being compromised before you do).

We know how important it is to keep your bank accounts secure. You don't have to do too much to give yourself strong protection, though. Just make sure you have great security software, bank with reputable institutions, and regularly look through your transactions and bank statements. **Just being vigilant will help you stay one step ahead of the cybercriminals.** Until next time, stay safe online!