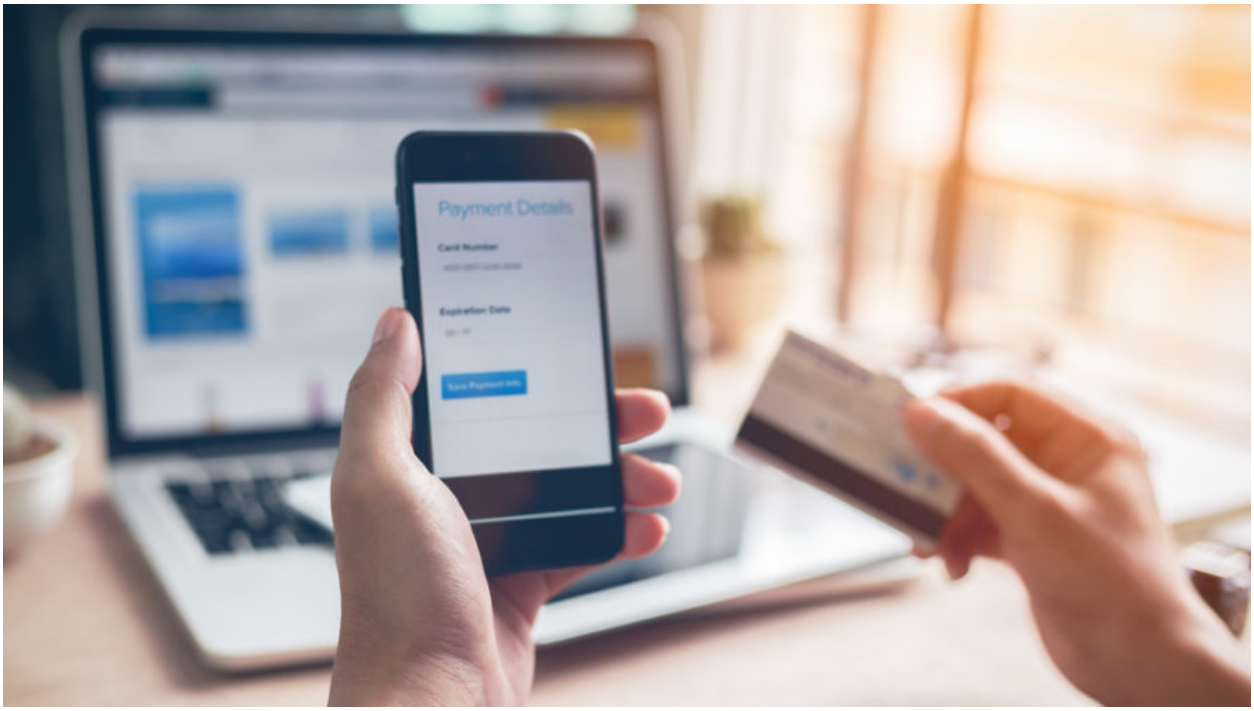
Important tips for safe online shopping post COVID-19

As more and more countries order their citizens inside in response to COVID-19, online shopping—already a widespread practice—has surged in popularity, especially for practical items like hand sanitizer, groceries, and cleaning products. When people don't feel safe outside, it's only natural they'd prefer to shop as much as possible from the safety of their own homes. Unfortunately, you can bet your last toilet paper roll that cybercriminals anticipated the rush and were ready to take advantage of our need to buy supplies of all kinds online.

Because we know how cybercriminals think and have already seen an uptick in web skimmers and coronavirus scams, we wanted to prepare our readers for a safer online shopping experience. We have rounded up some tips for staying secure, as well as some landmines to avoid during your online shopping spree.



Dangers to avoid while shopping online

There are a few dangers that always lurk for online shoppers, and some of them increase in severity during particular events, such as holidays or summer travel season, known shopping periods like Cyber Monday or Singles' Day, or tragic incidents,

including natural disasters and the current global pandemic. Here are a few red flags to watch out for:

Raised prices

It's only natural to expect a small raise in prices as some companies cope with economic fallout from closing brick-and-mortar shops and lack of personnel. Combine that with an increase in demand for specific items, plus the increased cost of delivery to compensate for added danger, and the totals at checkout are probably creeping up all over the place. But it's one thing to raise prices responsibly. It's quite another to price gouge, and cybercriminals and scammers are opting for the latter to profit from misfortune.

During times like these, it's easy to click "purchase" on the first webpage peddling scarce or highly sought-after commodities. For example, two brothers tried to make a fortune selling hand sanitizer for $70 per bottle. People were desperate enough to buy before the attorney general shut down the site. But don't fall for the hype. Take a deep breath and research an item before jumping at the first opportunity to purchase.

Pro tip: If a price seems wildly out of line, open up a new tab on your browser and search the item name and pricing. You can also check sites such as Tom's Guide or Consumer Reports for fair prices.

Delays in delivery time

If items are scarce, there may be a long waiting time before delivery. Know your rights in case a supplier can't deliver within the agreed time frame, and don't fall for scammers promising they can help you cut the line. Usually, you can claim a refund if the article doesn't arrive by the date you were promised. But a scammer couldn't care less about

your claims for a refund. They will make sure they are nowhere to be found when the claims come in and the going gets rough.

Pro tip: Search a website's customer service page to find out delivery and return policies before purchasing, especially items in short storage. Typically, these policies are found on shipping, support, help, or FAQ webpages.

Counterfeit goods

Selling counterfeit goods is another common type of web crime that will likely see an uptick during the coronavirus pandemic. From a photograph it is nearly impossible to tell whether an item is faux or the real deal. For all we know, the scammer could put a picture of the original on their site and ship you a cheap replica—or nothing at all. A good rule of thumb is: If it's too good to be true, it usually isn't.

Pro tip: Check the reviews of the seller, reseller, and product—not just on the site, but in a separate search. If someone has been duped before, chances are, they'll post pictures or a review.

Web skimmers

Ever since shelter-in-place orders have sent millions of shoppers online, the Malwarebytes threat intelligence team has noticed an uptick in the amount of digital credit card skimmers, also known as web skimmers. Web skimmers are placed on shopping cart pages and collect the payment data that customers enter when they purchase an item online.

Cybercriminals can hack the websites of legitimate brands to insert web skimmers, so avoiding resellers or little-known boutiques won't protect shoppers from web skimmers. Instead, consider using an antivirus with web protection or browser extensions that block malicious content.

Jérôme Segura, Malwarebytes Director of Threat Intelligence is an internationally renowned expert on web skimmers. He was kind enough to share some of his knowledge with us:

"The vast majority of people, including those familiar with computers, would not be able to see that an online merchant has been hacked and that a skimmer is going to harvest their information.

But there are certain things you can do to minimize risks. For example, check that the site looks up to date by looking at things such as copyright information. If it says something like Copyright 2015, this may be an indication that the site owner is not paying attention to details.

I also believe it's essential to use some kind of web protection. Based on our telemetry, we stop hundreds of attempts to steal credit card data on a daily basis by blocking malicious domains and IP addresses associated with web skimming infrastructure."

Pro tip: Keep an eye on your bank account for unexpected payments, and know what to do when your information has been stolen.

Recommended reading: [How to protect your data from Magecart and other e-commerce attacks]

Precautions and possible pitfalls

While not outright dangers, there are a few somewhat shady behaviors that could signal further trouble down the road. Here are a few you might want to avoid or consider when you consider online shopping.

Security certificates

A significant surge in the number of requested security certificates indicates that more fraudulent websites are being created. As we have mentioned before on the blog, the green padlock alone does not guarantee a safe site. Free or cheap security certificates are an indication that the site might be fraudulent or built without any attention to real security.

Use trusted sites and visit them directly, not through a search. Using legitimate sites with a good reputation does have obvious advantages. You know it's a real shop and they deliver on what they promise.

Pro tip: Bookmark favorite URLs to save on manually typing. By saving the URL rather than searching for a shop name, you are less likely to be fooled by impersonators.

Targeted ads

Targeted advertising should not be rewarded. Usually it's better to ignore it. Pretty much for the same reasons as above. Visit the site directly instead of clicking a link in your Facebook feed. Since many shops use cookies for targeted advertising, they will soon pick up that you are looking for a certain item and try to lure you to site by offering it to you in your timeline.

Pro tip: Consider purchasing insurance for high-value products. With insurance, you can at least get your money back if your purchase never arrives or is damaged or otherwise below expectations. Insurance does not have to be expensive. PayPal and many credit cards offer this service free of charge.

Information overload

Be wary of web shops asking you for information they don't need to service you. They might be up to no good. And even if they are not, they have no right asking you for details that are unnecessary for the shopping and delivery process. Even if they do not plan to sell your data to third parties, they may experience a breach and spill your personal information anyway.

Pro tip: Only fill in required sections of any data forms for an online purchase. And if a form starts asking for social security numbers, pet's names, or other weirdly personal information, do not enter the content and back out of the purchase.

Recommended reading: [10 tips for safe online shopping on Cyber Monday]

Preventative measures

As always, it's important to take the normal security precautions while shopping online. These include the following:

- Use up-to-date software, especially your operating system and your browser. Check that both are updated before you venture online.
- Disregard overly aggressive pop-ups, push notifications, and other annoying cries for attention. Usually, unsolicited advice in the form of persistent advertisements, browser extension downloads, coupon programs, and other assorted spam are aiming for trickery and not actually trying to help.
- Pay extra attention when using public Wi-Fi, and avoid making payments while you are on unprotected Wi-Fi.

- Where possible, use a VPN during online shopping. A good VPN will encrypt the traffic between you and the online shop, so nobody can spy on it.

Be Careful, Stay Safe, Be Confidant Everyone!