April 2017

National KE-CIRT/CC Information Security Tip of the Week

ONLINE SHOPPING

Online Shopping Security Threats

Abstract

Online Shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the Internet using a web browser

Shopping websites like Jumia and OLX Kenya are beginning to sell not only appliances, electronics and furniture but even groceries, food and travel deals.

These improvements have greatly increased online traffic and with this growth comes an added risk cyber attacks. It is important to take steps to protect yourself and your information while buying or selling online.

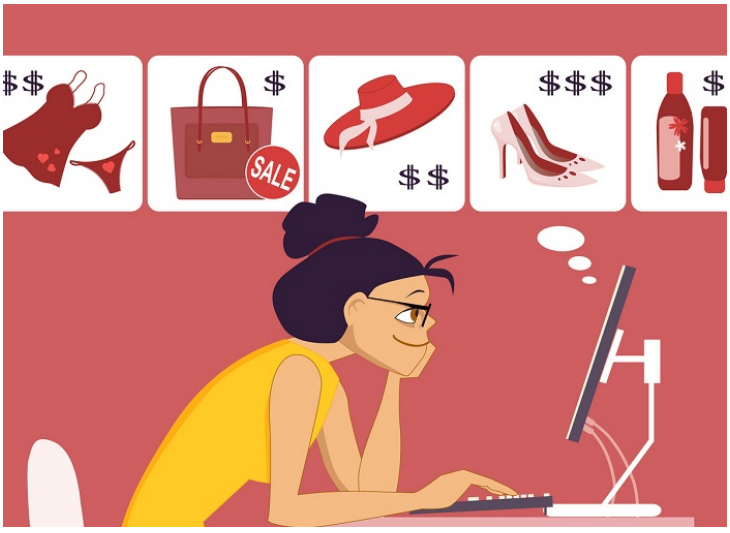
;

Tips for Safe Online Shopping

Before you go for online shopping make sure your PC is secured with all core protections like an antivirus, anti spyware, firewall, system updated with all patches and web browser security with the trusted sites and security level at high.

Make sure you at least have an updated browser when you order things online. This will help secure your cookies and cache, while preventing a data leakage.

Before you buy things online:



- Research about the website that you want to buy things from since attackers try to come up with fake websites that appear to be legitimate.
- Make a note of the telephone numbers and physical address of the vendor and confirm that the website is a trusted site. Search for different websites and compare the prices. Check the reviews of consumers and media of that particular web site or merchants.
- Online shops, particularly those in the fashion niche, take great of the design and usability of their websites. If it has a horrible design, it is most likely fake.
- When prices are ridiculously low it may be a fake site. If it's too good to be true, it
usually is fake.

If you are ready to buy something online:

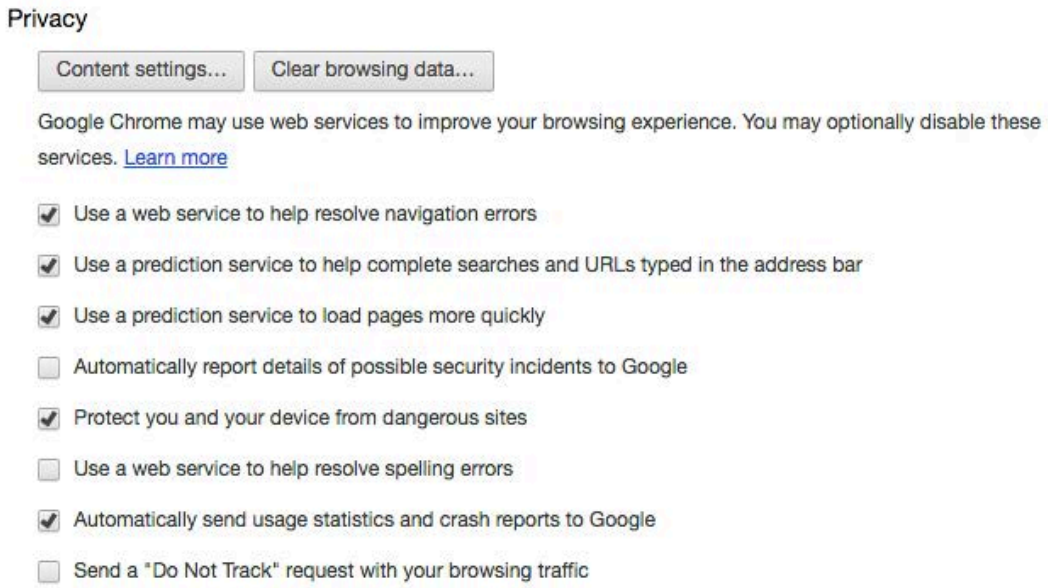
- Check whether the site is secure by confirming the url has features like https or a padlock icon on the browser address bar or at the status bar before proceeding with the financial transactions.
- Strange URL's such as "prada-at-awesome-price.com" or "the-bestonlineshopping.com"
- Fake Facebook accounts have been known to mimic popular online shopping webpages such as "Jumuia Kenya" instead of "Jumia Kenya".

After finishing the transaction:

- Take a print or screenshot (***Ctrl-PrntScrn*** (Windows) or ***Command-Shift-3*** (Mac) of the transaction records and details of product like price, confirmation receipt, terms and conditions of the sale.
- Keep the receipt for your purchase, just in case you need to confirm it again, as well as for warranty and return issues. If you want to get rid of receipt, make sure to destroy it completely, so that any possible identity thief won't be able to find any little information about you.

- Immediately check the credit card statements as soon as you finish the transaction. In the event there are any anomalies in the transaction, notify the bank or any concerned authorities.
- Whenever possible, try to activate two-factor authentication payment methods.
- Be sure to keep confirmation numbers and emails for any online purchases you may have done.
- Notify your credit card issuer of any address change. Doing so will prevent them from sending sensitive files to the previous address.

After finishing your online shopping clear all the web browser cookies (***Ctrl-Shift-Delete*** (Windows) or ***Command-Shift-Delete*** (Mac) and turn off your PC since spammers and phishers will be looking for the system connected to the Internet and try to send spam e-Mails and try to install the malicious software that may collect your personal information.



Have the above security tips in mind when securing your computer system. Report any cybercrime incident/activity to incidents@kecirt.go.ke. www.ke-cirt.go.ke

COMMUNICATIONS AUTHORITY OF KENYA

Ikenya

KENYA VISION 2030