Online Shopping Safety Guide: 15 Tips That You Should Remember

People prefer online shopping nowadays because it's very convenient — all it takes are a few clicks in front of your computer or several taps on your phone — to order a product and have it delivered straight to your home. No need to stress yourself on what to wear to the nearest mall or retail store.

You could also argue that it's safer — since you no longer run the risk of having your wallet stolen — but online shopping requires you to share your personal information and credit card details. And where there's money, there are also people with malicious intent.

These fifteen online shopping safety tips will help you prepare against cybercriminals lurking on the Internet.

The online version of this article can be found here:
https://dealhack.com/blog/online-shopping-safety-guide

1: Beware of fake shopping websites

People who don't shop in safe online stores like Amazon and eBay should definitely watch out for fake shopping websites. Your computer can get infected by malware from these websites when you click on unsafe links. Unsuspecting shoppers who checkout their order at a fake website will compromise their full name, home address, credit card number, and credit card security code. The hackers who retrieve your personal data can then use it to commit crimes such as identity theft and credit card fraud.

Common signs that a website is fake:

- The URL is suspicious. If you come across websites that are named as "prada-at-awesome-price.com" or "the-bestonlineshopping.com", chances are they're not legit.
- Poorly writing. A legit online shop uses proper grammar and vocabulary to improve the SEO and readability of its webpage. Always be suspicious of websites that have many grammatical errors in the product descriptions.
- Poor design/layout. Online stores, especially those in the fashion or electronics niche, need to be well-designed to attract customers. If a website that sells clothing or gadgets has a poor user interface, most likely it's not legit.

- Suspicious product list. Read the “About Us” page of an online shop and compare what it says to the products that they sell. If a clothing website has car accessories in its product selection, it’s safer to buy somewhere else instead.

- Suspicious contact information. A legit online store usually uses a business email address (e.g. support@ebay.com) for its customer service. Suspicious websites use personal email addresses such as “ebaysupport@gmail.com”. When in doubt, read the information that is found in a website’s “Contact Us” page.

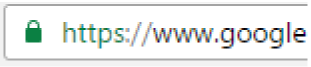
- Product prices are suspiciously low. Online shoppers always find the lowest possible price for any product. This makes it easy for unsuspecting shoppers to get scammed by fake websites. If you found an iPhone 12 for sale at $150, most likely the website is not legit.

Always keep these basic tips in mind if you want to buy products from online shops that are actually legit.

2. Shop at websites that are properly encrypted

Shopping online will always require you to share personal information on the Internet. Online stores that use SSL (secure sockets layer) encryption are safe to browse. Encrypted data have a very low risk of getting stolen by malicious hackers.

Check the URL in the address bar. If it has a lock symbol and the keyword https:// then it means the website uses SSL encryption. For example, when you visit Google this is what you can see in the address bar:



🔒 https://www.google

Fake online shops are not SSL- encrypted, so always read the address bar before you continue to browse any website.

3. Use secure Internet connections

Wi-Fi is accessible nowadays, but that doesn’t mean it's always safe. Connecting to an unsecured network lets a malicious hacker intercept all your Internet traffic. Everything that you input online can be tracked and stolen, especially your credit card information, personal address, and passwords.

Here are the common signs that you might be using an unsecure Wi-Fi connection:

- Open connection with no password protection. It doesn’t matter how many people are using the Wi-Fi network; if it does not have a password, that means it’s a nice target for even the simplest cybercriminals. Always do your online shopping in secure connections!

- It uses WEP/WPA encryption. Both are simple encryption languages that any competent hacker can infiltrate with ease. Networks that are encrypted with WPA2 AES are safer. Although WPA2 AES-encrypted connections are not immune to very expert cybercriminals, they provide a better layer of protection over those that use WEP or WPA.
- The Wi-Fi router is in a public area. Cybercriminals are more likely to tamper Wi-Fi routers that are exposed in public places. Bars and restaurants that have a Wi-Fi hotspot are always full of people that connect to their network. Skilled cybercriminals can hack into open networks even if they are password-protected, so it’s best to avoid online shopping while connected to public Wi-Fi.

4. Update your web browser and operating system

Online shopping can be done on any device that can connect to the Internet. Whether you’re using a phone, tablet, or computer, always keep its operating system (OS) up-to-date. Apps and devices that are updated to their latest versions have a higher chance of protecting your personal data whenever you shop online.

You can automatically download and install updates on your computer, but it’s completely optional. Some updates do not improve your computer’s antimalware protection, so you don’t always have to install every single update. Instead, you can choose manual download and installation of updates to reduce waiting time for your OS to get ready.

For smartphones, firmware updates generally take less time compared to those on computers. These updates are usually the important ones, so make sure to install them as soon as you can.

Use reliable internet browsers such as Chrome, Edge, Firefox, Opera, and Safari. Whatever browser you choose, always update it to protect your search history and saved passwords.

5. Secure your bank account

Cybercriminals are after your credit card information, and the best way to acquire that is by hacking into online stores. Data leaks are not always the fault of the customers. There are times when credit card companies get hacked and cybercriminals are able to steal important personal information.

Always be on the lookout for suspicious activity when it comes to your bank account. These financial safety reminders should be kept in mind:

- Never tell your credit card number to anyone.
- If you ever keep a copy of your PIN number, don’t put it in the same location as your credit card.
- Whenever you change your home address, notify the bank that issued your credit card as soon as possible.
- Enable two-factor authentication for payment methods if they are available.
- Keep the confirmation numbers and emails for all your online purchases.
- If you ever lose your credit card or even think that you only misplaced it, don’t hesitate to lock it. It’s easier to replace a lost credit card than lost money.

6. Use a VPN when browsing the Internet

If you can’t avoid browsing on a public Wi-Fi network, use a Virtual Private Network (VPN) for an added layer of security. VPNs establish an encrypted connection between your computer and the Internet server. Any cybercriminals that are tapped into the public Wi-Fi will have a difficult time intercepting your data traffic. Many VPNs are available for free, so make sure to read up on the reviews for each brand before choosing a go-to VPN whenever you surf the web in public spaces.

7. Install multiple protective measures on your device

Antivirus programs keep your computer or phone safe by scanning your files for malware intrusions. For PC users, Windows Defender is free and highly effective as long as you update it regularly. If you want antivirus programs with additional security features, Avast, McAfee, and Norton are popular choices for different devices. These programs have free versions but they also offer discounts regularly for their paid subscriptions.

One major disadvantage of an antivirus program is that it’s only a reactive solution. It only becomes effective after your PC has been infected by malware.

Choosing only one security measure against cybercriminals may not be enough. Add an extra layer of security to your device by using a tool that scans websites and files for incoming malware. The advantages of these programs are:

- Advanced traffic scanners filter incoming and outgoing traffic to your device and detect any signs of potential malware.

- It will scan a website for embedded malware and block it from loading in case it finds one.
- Malware that still found their way to your device will be effectively removed.

8. Use a password manager to protect your personal accounts

We love to reuse the same password for multiple accounts because it’s very convenient for most us. Whenever we create an account for an online store, we usually use the same password we have for our email and social media accounts. But using the same password can be dangerous.

Writing down your password is not recommended. So if you’re forgetful or just like to keep things organized, using a password manager such as LastPass or Dashlane is a fast and secure way of logging in to different websites. Also try to create stronger passwords whenever possible, and avoid predictable passwords such as your birthday and name.

9. Keep an eye out for common hacker tricks

Having the right security programs will go a long way in improving your safety when buying things online.

But what will really take your internet shopping to the next (security) level is a good understanding of cybersecurity threats combined with a few common sense rules on what you should and should not do online.

Here just a few relevant online shopping safety tips:

- Avoid clicking on suspicious links especially in pop-ups or emails.
- Before using free software, search them on Google to check if they are legit.
- Report websites that are fake or have offensive content.
- Mark unwanted and suspicious emails as “spam” and never reply to them.
- Never provide more information than what is required to complete an online purchase.

Once you know the tactics that hackers usually use, you can avoid them entirely. This makes it harder for them to infiltrate your online accounts.

10. Never click on spam or phishing emails

Phishing emails are cunningly designed to look like legitimate emails from trusted businesses.

The most common way for phishing emails to gather plenty of clicks is when they are attached with a fake offer for an appealing product. Impulsive shoppers are prone to click “Buy now” or “Order now”. Many malware attacks begin with phishing emails.

Many people click on the “Unsubscribe” button when they don’t want to receive certain emails anymore. Cybercriminals take advantage of this knowledge to create phishing emails with a fake “Unsubscribe” link.

If you come across a suspicious email, mark the email as spam. This effectively removes the email from your inbox. The sender will also be blocked from giving you additional spam emails.

11. Monitor your transactions and hold on to your receipts

Shopping responsibly means that you keep a record of every product you bought online. This includes the date of purchase, price, and the website where you ordered them. Every detail counts, no matter how minor you think it may be.

Compare the cost of each product and the amount charged to your credit card for every purchase. You want to make sure that you were not overcharged for a particular order without prior knowledge.

Once you successfully place an order, keep the order confirmation number and receipt. These are usually sent to the email address that you're provided upon ordering. Receipts are important for order tracking and other possible concerns such as warranty and returns.

If you no longer need to keep some receipts, don’t just leave them lying around in your house. Instead of just throwing them in the trash, shred or burn them if possible to leave no trace.

Digital receipts or bank statements in PDF or Word format that are removed from your PC and can still be recovered again through console commands or “Restore Previous Versions”. Use a file shredder app to make these files permanently unrecoverable.

12. Be mindful of what personal info you share on shopping websites

Online stores only require the following to successfully process your order: payment information and shipping location.

Payment information includes your credit card number, expiry date, security code, and billing address. Be careful about saving payment methods to online store accounts because all it takes is one data leak and your finances will be in danger. Shipping location includes your street address and zip code. Some stores may also ask for your email address and phone number but these are only needed for tracking your orders.

It’s best to avoid shopping at stores that ask for the following information: social security number, date of birth, and bank account number.

Cash on delivery (COD) is the safest mode of payment because you directly give your money to the person who will be handing you the package. This eliminates the need for you to input your credit card data online. If COD is available at the store that you’re shopping, it’s best to choose that option.

If you prefer not to give away the address to your home or office, you can ask the store if they allow orders to specific delivery points such as P.O. boxes. That way, you can pick up your order at a safe location and still manage to keep your privacy intact.

13. Avoid keeping too much personal information on your smartphone

These days, everybody stores a lot of important personal information on their phone, and most of us rarely take the time to secure them. These devices are now much less about calling people, and more about photos, social media and whatnot.

Increasingly, people shop online using their smartphone, but this carries its own risks. Fake online shops can infect your smartphone with malware, and then have access to information such as phone numbers, notes, photos, and even app contents.

For this reason, we recommend you keep as little information as possible on your phone, and instead rely on offline storage or cloud solutions.

14. Download reliable mobile shopping apps

Mobile security used to be safer than desktop or laptop security, but that’s no longer the case today. Majority of smartphones use either Android or Apple operating systems, and cybercriminals have already figured out how to hack into these devices.

If you prefer to shop on mobile apps instead of your computer, here are some useful tips:

- Download apps from secure digital marketplaces like Google Play, Apple App Store, Windows Store, and Amazon Appstore.
- Major retailers such as eBay, Amazon, and Walmart have their dedicated mobile apps. Download them if you want an easier shopping experience.
- Always keep your frequently used shopping apps updated to their latest versions.
- Take note of the app's permissions. If a shopping app requires your phone's contact list, messages, or microphone, don't allow access. These features are not required for online shopping.
- Read the customer reviews of a shopping app before you download it so you can be informed of its pros and cons.

15. Shop using a credit, not debit

The simplest explanation is that debit cards contain your personal money while credit cards use the bank's money. Credit cards are equipped with extra-legal measures so they are safer to use for online shopping compared to debit cards.

Here are two major reasons why you should use credit cards for online shopping:

- If you suspect any fraudulent transactions using your credit cards, you won't be liable for losing the bank's money as long as you report it as soon as possible.
- Credit cards give you leverage if ever you need to dispute transactions with a seller. The money you paid for purchasing a product using a credit card will not be counted against you until due process is complete. In contrast, paying with a debit card means that you can only get your money back if the seller agrees to it.

Credit cards are worth getting if you're sure to be making plenty of online transactions. Banks are very protective of their credit cards since technically it's their money on the line instead of yours. Keep your debit card safe from malicious hackers.

Conclusion

The rise of digital marketing allowed shoppers to access their favorite stores through their phones and computers. Online shopping safety is a growing concern for e-commerce companies and consumers alike. The former wants to protect their reputation and business, while the latter wants to know that their money and personal info are safe.

Web and app developers continue to create additional security measures to improve online security. You should also do your part and stay informed on the best ways to protect your personal information from malicious hackers.

The online version of this article can be found here:
https://dealhack.com/blog/online-shopping-safety-guide

d