

Mankato Computer Technology Presents:

COMPUTER UNIVERSITY: BUYING ONLINE

Monday, October 18

The pandemic has made buying items online more necessary. And you're probably buying things you never thought you would buy online. With new purchases come new concerns. Some popular sites will be discussed.

<https://www.bustle.com/p/11-things-you-need-to-know-about-online-shopping-to-get-your-full-moneys-worth-43372>

Multi-factor authentication

- ▶ *when a user must provide two or more pieces of evidence to verify their identity to gain access to an app or digital resource. Multi-factor authentication (MFA) is used to protect against hackers by ensuring that digital users are who they say they are.*
- ▶ an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:
- ▶ MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.
- ▶ A *third-party authenticator* (TPA) app enables two-factor authentication, usually by showing a randomly generated and frequently changing code to use for authentication.

BUYING ONLINE

- ▶ There's every reason in the world to shop online.
- ▶ The bargains are there. The selection is mind-boggling. The shopping is secure.
- ▶ Shipping is fast. Even returns are easy, with the right e-tailers.
- ▶ Shopping has never been easier or more convenient for consumers.
- ▶ And in the age of COVID, it's safer than going out even if you're fully masked and gloved.
- ▶ But what about the bad guys? It happens. The FBI's own [Internet Crime Complaint Center \(IC3\)](#) says the number one cybercrime of 2019 in half the 50 states was related to online shopping: [non-payment for or non-deliver of goods purchased](#).
- ▶ Stay calm. While somewhat alarming, these stats should *not* keep you from shopping online. You simply need to use some common sense and follow practical advice. Here are basic guidelines; use them and you can shop with confidence.



Things You Need To Know About Online Shopping

- ▶ Again, shopping on the internet is convenient, quick, and you can do it from the comfort of your very own couch. Just keep these things in mind when you're adding items to your (virtual) shopping cart.

Things You Need To Know About Online Shopping

- ▶ Shopping online is fast and easy, but those very qualities can make it dangerous.
- ▶ “The convenience of online shopping is also a pitfall,”
- ▶ “We can do it wherever and whenever we want. To go out and shop in a store takes more time and planning which can often serve as a barrier for impulse purchases and buying things we otherwise wouldn't.”

Stay safe.

- ▶ When you shop online, you transmit sensitive info like your credit card number — so it's important to be careful about where you shop and the information you give out.
- ▶ [*PC Magazine*](#) suggests that, at the very least, you should only shop on websites that start with “https://,” rather than “http://.”
- ▶ That extra letter means that the website has an added layer of security; you should also keep an eye out for the little lock icon that shows up when you're on a secure website.
- ▶ Stick to websites you know, and steer clear of websites that ask you for extra identifying information. (An online shop should never ask for info like your Social Security Number, for instance).
- ▶ In general, if a website seems fishy to you, don't give it your credit card information.

Use Familiar Websites

- ▶ Start at a trusted site.
- ▶ Search results can be rigged to lead you astray, especially when you drift past the first few pages of links.
- ▶ If you know the site, chances are it's less likely to be a rip-off.
- ▶ We all know Amazon.com carries everything under the sun; likewise, just about every major retail outlet has an online store, from Target to Best Buy to Home Depot.
- ▶ Beware of misspellings or sites using a different top-level domain (.NET instead of .com, for example)—those are the oldest tricks in the book.
- ▶ Yes, sales on these sites might look enticing, but that's how they trick you into giving up your info

Check the Seller

- ▶ If you're wary of a site, perform your due diligence.
- ▶ The Better Business Bureau has an [online directory](#) and a [scam tracker](#).
- ▶ Yelp and Google are full of retailer reviews. Put companies through the wringer before you plunk down your credit card number.
- ▶ There's a reason that non-delivery/non-payment is the most common cybercrime complaint: it hurts when that happens, financially and emotionally.
- ▶ That said—online reviews can be gamed. If you see nothing but positive feedback and can't tell if the writers are legitimate customers, follow your instincts.
- ▶ If nothing else, make absolutely sure you've got a concrete address and a working phone number for the seller.
- ▶ If things go bad, you have a place to take your complaint. In fact, call them before you order so you can clarify a return policy and where to go with any issues after the purchase.

Look for the Lock

- ▶ Never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed—at the very least.
- ▶ You'll know if the site has SSL because the URL for the site will start with **HTTPS**—instead of just HTTP.
- ▶ An icon of a locked padlock will appear, typically to the left of the URL in the address bar or the status bar down below; it depends on your browser.
- ▶ HTTPS is standard now even on non-shopping sites, enough that Google Chrome flags any page without the extra S as "not secure." So a site without it should stand out even more.

Don't Overshare

No online shopping e-tailer needs your Social Security number or your birthday to do business.

However, if crooks get them and your credit card number, they can do a lot of damage.

The more scammers know, the easier it is to steal your identity.

When possible, default to giving up as little personal data as possible. Major sites get breached all the time.

Create Strong Passwords

- ▶ PCMag asked readers if they frequently changed their passwords.
- ▶ Eleven percent claimed they did it every day, but those people are either paranoid, liars, or paranoid liars.
- ▶ The vast majority only change a password to protect privacy a few times a year (27 percent) or more likely, never (35 percent).
- ▶ If you're going to be like the latter group, we will again beat this dead horse about making sure that you utilize uncrackable passwords.
- ▶ It's never more important than when banking and shopping online.
- ▶ Tips for [creating a unique password](#) can come in handy during a time of year when shopping around probably means creating new accounts on e-commerce sites.
- ▶ Even your perfect password isn't perfect. The smarter move: use a [password manager](#) to create uncrackable passwords for you. It will keep track of them and enter them, so you don't have to think about it.

Use a Password Manager

<https://www.cnet.com/tech/services-and-software/best-password-manager/>

- ▶ LastPass
- ▶ Blur
 - ▶ Abine's Blur is a browser add-on that acts as a basic password manager and oh so much more. For \$39 a year, it'll let you shop without revealing anything about your actual self—no emails, phone numbers, or even credit card numbers. It's one of the most impressive online privacy solutions we've ever seen. [Read full review.](#)
- ▶ **Bit warden**
- ▶ **1Password**

Check Statements Regularly

- ▶ Don't wait for your bill to come at the end of the month. Go online regularly, especially during the holiday season, to view electronic statements for your credit card, debit card, and checking accounts. Look for any fraudulent charges, even originating from payment sites like [PayPal](#) and [Venmo](#). (After all, there's more than one way to get to your money.)
- ▶ You should definitely only buy online with a credit card. If your debit card is compromised, scammers have direct access to your bank funds. Any seller that wants a different kind of payment, like wired money, is a big red flag. The [Fair Credit Billing Act](#) ensures that if you get scammed, you are only responsible for up to \$50 of credit card charges you didn't authorize. There are protections even if you're not happy with a purchase you did make.
- ▶ If you see something wrong, pick up the phone to address the matter quickly. In the case of credit cards, pay the bill only when you know all your charges are accurate. You have 30 days to notify the bank or card issuer of problems, however; after that, you might be liable for the charges anyway.

Inoculate your Computer

- ▶ Swindlers don't sit around waiting for you to give them data; sometimes they give you a little something extra to help things along.
- ▶ You need to protect against [malware](#) with regular updates to your [antivirus program](#). Better yet, pay for a full-blown [security suite](#), which will have antivirus software, but also will fight spam, [spear-phishing](#) emails, and phishing attacks from websites (the latter two try and steal your personal info by mimicking a message or site that looks legit).
- ▶ Remember, it's not enough to have it installed. Make sure your anti-malware tools are always *up to date*. Otherwise, they can let in any new threats—and there are always new threats.

Privatize your Wi-Fi

- ▶ If you're shopping via a public hotspot, stick to known networks, even if they're free, like those found at Starbucks or Barnes & Noble stores.
- ▶ Any of the providers in our roundup of the [Fastest Free Nationwide Wi-Fi](#) can generally be trusted, but you should probably also use a [virtual private network](#) (VPN) to be safe ([here's why](#)).
- ▶ For more, read our [Tips for Public Wi-Fi Hotspot Security](#).

Avoid Shopping in Public

- ▶ What about using your own laptop to shop while you're out?
- ▶ It's one thing to hand over a credit card to get swiped at the checkout, but when you have to enter the credit card number and expiration date and 3-digit code on the back into a shopping site while sitting in a public cafe, you're giving an over-the-shoulder snooper plenty of time to see the goods.
- ▶ Think like a gangster: Sit in the back, facing the door. Use sites that you trust that already have your credit card stored, so you don't have to pull it out for more than a latte.
- ▶ Better yet: stay home when online shopping.

Think Mobile

- ▶ There's no real need to be any more nervous about shopping on a mobile device than online.
- ▶ Simply use apps provided directly by the retailers, like Amazon and Target, even McDonalds or Chipotle.
- ▶ Use the apps to find what you want and then make the purchase directly, without going to the store or the website.

Skip the Card, Use the phone

- ▶ Paying for items using your smartphone is pretty standard these days in brick-and-mortar stores, and is actually even more secure than using your credit card.
- ▶ Using a [mobile payment app](#) like [Apple Pay](#) generates a one-time-use authentication code for the purchase that no one else could ever steal and use.
- ▶ Plus, you're avoiding [card skimmers](#)— you don't even need to take your credit card with you if you only go places that accept phone-based payments.
- ▶ How does that matter if you're online shopping?
- ▶ Many a phone app will now accept payment using Apple Pay and [Google Pay](#). You just need your fingerprint, face, or passcode to make it happen instantly.

Count the Cards

- ▶ When it comes to gift cards, stick to the source when you buy one; scammers like to auction off gift cards on sites like eBay with little or no funds on them.
- ▶ There are many gift card "exchanges" out there that are a great idea—letting you trade away cards you don't want for the cards that you do—but you can't trust everyone else using such a service.
- ▶ You might get a card and find it's already been used.
- ▶ Make sure the site you're using has a rock-solid guarantee policy.
- ▶ Better yet, simply go directly to a retail brick-and-mortar store to get the physical card.

Avoid counterfeits and scams.

- ▶ As the saying goes: If it seems too good to be true, it probably is.
- ▶ Counterfeits are rampant online, even on well known sites like Amazon; in 2016, [Birkenstock even pulled its products](#) from the mega-retailer because so many third parties were using Amazon to sell fakes.
- ▶ It can be difficult to spot fakes online, but use common sense: Buy directly from brands' online stores (rather than third parties), and be suspicious of prices that seem unrealistically low.
- ▶ Again, if it feels "off," shop somewhere else.

Things You Need To Know About Online Shopping



In 2016, a yearly survey by comScore and UPS found that, for the first time, people were doing more of their shopping online than in person.



And it's no surprise: Shopping online is fast, economical, and incredibly convenient.



However, there are a few things you should know about online shopping before you set yourself loose on the internet marketplace.



A savvy online shopper can save time and money, but it's important to be aware of the risks of shopping from your computer or smartphone.

Some days and seasons are better times to shop online than others.



Prices and discounts fluctuate throughout the year.



According to Lifehacker, you're most likely to find the most discounts in November and January and on Tuesdays and Thursdays.



March is the worst month for finding discounts – so if you're thinking of making a big purchase online, you may want to wait a few weeks.

Things You Need To Know About Online Shopping

- ▶ If you're trying to stay on budget, shopping online may be your best friend.
- ▶ "It can be easier to stick to a plan,"
- ▶ "When you have a plan and are searching for a specific item, shopping online can make it easier to avoid distractions, depending on the site. For example, if you are grocery shopping online, you might type in each item on your shopping list into the search bar and then choose which you want. When we're in the grocery store, we see many things that aren't on our list and might decide to buy them anyway. In this case, we're more prone to impulse."

You can save money by searching for coupons before you buy.

- ▶ Before you buy anything online, do a quick google to see if there are any discounts or coupons available.
- ▶ Just search the name of the company where you're shopping and "coupon 2021"; there's a good chance you'll find a coupon code to apply to your purchase.
- ▶ I've gotten *a lot* of free shipping this way, and every little bit helps, right?

- ▶ When you're shopping online, keep an eye out for extra charges that may crop up at the last minute — that great “deal” you're getting might not be so great when you add up the total cost.

**Be on the
lookout for
hidden or last
minute fees.**

Be careful about signing up for newsletters and email lists.

- ▶ When you go onto a company's website, you'll often get a pop-up asking you to sign up for the company's newsletter and an offer of a coupon in exchange (usually for around 15 percent off).
- ▶ In many cases, you'll automatically be signed up for email lists when you purchase something online or from a store.
- ▶ If you know that you're going to buy something, taking advantage of these coupons can be a way to save money, that company emails often do more harm than good.
- ▶ "These daily or weekly emails prompt us to check out a new product or sale when we otherwise wouldn't,"
- ▶ "It can create a want or need where there wasn't one and this can cause us to spend more and yearn for more.
- ▶ Unsubscribing from email lists is a great way to decrease your desire to shop."

Read the reviews!

- ▶ Product reviews can be incredibly helpful when you're making online purchases.
- ▶ They can tell you if the product looks the way it does in photos or how it holds up over time; and, for apparel especially, they can give valuable info about fit.
- ▶ Keep an eye out for patterns: If reviewer after reviewer says that a shirt runs small or that a chair that looks blue online is actually gray in person, believe them.



Complain Loud and Proud

- ▶ Don't be embarrassed if you get taken for a ride while online shopping.
- ▶ Instead, get very, very *mad*. Complain to the seller.
- ▶ If you don't get satisfaction, report it to the [Federal Trade Commission](#), your [state's attorney general](#), even the [FBI](#).
- ▶ That's probably going to work best if you buy in the US, rather than with foreign sites.
- ▶ If you're going to get scammed, try to get scammed locally... or at least domestically.

But also be skeptical of the reviews.

- ▶ Customer reviews can be super handy, but sometimes they can also be super fake.
- ▶ In fact, since 2015, [Amazon has sued over 1,000 people](#) involved in fake product reviews on its site, including sellers that have paid for fake reviews and reviewers who have made them.
- ▶ Practice some healthy skepticism of online reviews. [NBC News suggests](#) that to spot fakes, keep an eye out for reviews that are hyperbolically enthusiastic (i.e. “This travel iron has CHANGED MY LIFE.”) or overly specific (meaning that, if a reviewer sounds like he or she is parroting a press release, something is off).
- ▶ If a product has a lot of reviews and they are *all* positive, that should raise some eyebrows, too.

Even if you're shopping in *virtual* stores, you're spending *real* money.

- ▶ I know that I'm pointing out the obvious — *of course* you're spending real money when you're shopping online — but I've found that shopping online has a magical ability to make me... forget.
- ▶ At least temporarily. I'm as guilty as anyone of feeling like the money I spend online doesn't really "count," *especially* on sites like Amazon, where I can hit "Buy now with 1-Click" and not even have to go through the process of getting out my credit card and entering the numbers.
- ▶ Shopping online is extremely convenient, but that very convenience can be dangerous for a budget.

- ▶ Shopping online allows you to check out prices from multiple retailers to make sure you're getting the best deal.
- ▶ You can get started comparing prices on sites like [Google Shopping](#), [Shopping.com](#), and [Nextag](#). (There are a bunch of [price comparison apps out there](#) that will let you compare prices when you're shopping in person, too.)

**Price
comparison
websites and
apps can help
you find the
best price.**

Incentives are designed to get you to impulse buy.

- ▶ Amazon and other websites will sometimes offer free shipping— *if* you spend above a certain amount.
- ▶ It's a strategy intended to get people to buy more than they originally intended, and it works: A [survey by The Yankee Group](#) found that almost half of shoppers made impulse purchases due to the promise of free shipping.
- ▶ Sometimes those free shipping offers can be good deals — *if* you'd already planned to spend above the threshold — but be careful that you don't fall into the trap of spending cash you can't afford on stuff you don't need.

In Conclusion



Be Safe.



Still not sure if you should make an online purchase? Use the “48 hour rule.”



When you find something you want to buy, wait 48 hours before hitting “Checkout.”



If you still want the item after a couple of days, go for it — but there’s a good chance that you’ll simply lose interest after you cool off.



“Often you’ll find that it’s not even worth going back for once you’re out of the moment.”