How to shop online privately

Intended purpose:

The purpose of this How-To Guide is to share strategies to minimise how much of your data is shared with third parties when transacting online. For most people these third parties are primarily their bank and the company or person who is the seller in the transaction. By enacting these strategies, you will reduce the risks posed to you in the event the company or person you're buying from has their data breached by bad actors.

Who will this help?

Most people who are simply privacy conscious and want to make changes to service this will get something out of this How-To Guide, however more specifically:

- People who have been burned by having their private information fall in the hands of a bad actor. Typically, they are not at fault, but the company they did business with had poor cybersecurity infrastructure and failed to protect customer information adequately.

- High-net-worth individuals with significant assets who wish to keep their transactions private. A record/s of purchasing high value products or services can make someone a target of:
  - Opportunistic lawsuits
  - Requests for financial support
  - Bad actors seeking a ransom (threat of doxing, false accusations, phishing attacks, reputational damage, kidnapping, etc)
  - Unscrupulous investors spruiking various investment opportunities
  - Other similar unwanted attention based on their financial state not being private

- People who wish to make donations anonymously

Disclaimer:

Reference to companies or providers in this guide is of a **general nature only**. Whilst Privacy Rightfully has vetted their legitimacy for inclusion in this guide to the best of our ability, we cannot guarantee they are an appropriate service for everyone. **We do not advocate using or not using any company or provider listed**, please conduct further, detailed research to see if they are right for you.

Part One: Protect your data

This first part focuses on the typical information you need to provide when shopping online. The goal here is to get your purchase delivered whilst providing the least amount of data or accurate data as possible.

Open a 'burner' email account

Set up a burner email for online purchases, most people have an email address in the format: firstname.lastname@email.com some even put the last two digits of their year of birth after their last name. This is already a lot of information handed over too easily, and being an email address, **it typically isn't as well protected** by online merchants as payment information is required to be.

If your name is Rose Stewart and you were born in 1962, keep your rose.stewart62@email.com strictly for family and friends – no online shopping or subscriptions. For shopping and subscriptions set up, say, mary.spencer72@email.com for example.

For high value or highly sensitive or private purchases consider opening a burner email like this simply for that transaction. However, for most folks opening a new email account for every individual purchase is not viable.

Hide your IP address

When logging into your burner email or visiting the website you are purchasing from, conceal your IP address with the Tor browser or a quality VPN.

Postal address

The best option for delivery is if you have a PO Box or own a business – send your online purchases there – anything to **avoid providing your residential address**. Obviously, this is to minimise the amount of times and places your home address is recorded on the internet, but it has a secondary reason some people don't often consider. It also reduces the frequency a courier will attempt delivery to your home which means the odd unscrupulous one can't identify a pattern of time when no one is home to consider a burglary.

Enter only what's required

When completing the shipping details, complete only what is required by the seller (typically marked with a *). If the seller has a box for date of birth or mobile number and it isn't required – don't provide it. **Provide the only bare minimum information required**.

Remember using bogus names, dates of birth, or other information – **do not use someone else's who you know** (a real person). This could cause you legal issues.

Part two: How to pay

The next step is to secure your financial accounts by reducing the use of your true account numbers and credit card numbers as well as increasing the links / steps back to them.

Prepaid / gift cards

The most anonymous way to pay is using an **anonymous prepaid card**, these are available for purchase at many stores and are typically used as gift cards. Ensure you purchase it using cash and dispose of it after each use (do not recharge it as it creates a data trail to your bank account).

Pros	Cons
Personal details are not needed as the money is taken when the card is purchased (as opposed to when it is used)	The inconvenience of having to go out and purchase one each time you want to buy something online
Very anonymous provided you purchase it with cash	Some may require personal information to activate the card
Easy to access with widespread availability to purchase	Not accepted by all online merchants
	Being left with unusable balances
	Typically limited to $500

It may not be practical for every online purchase you make so consider this payment option exclusively for personal or sensitive purchases.

Paysafecard

By purchasing a Paysafecard with cash you can make anonymous online payments. Vouchers are sold in retail stores and come with a long 16-digit PIN.

Pros	Cons
Does not require a credit card or bank account if you purchase with cash	Not widespread – it can be difficult to find retailers selling them.
Can combine up to 10 Paysafecards for larger purchases	Not widely accepted – it can be difficult to use them with online gaming and gambling the most common uses currently
Very anonymous	

Other payment options

The following list features payment options which are **partially but <u>not totally</u> anonymous** which we've included for two reasons. The first is they speak to our mantra of helping people make small changes which make them a more difficult target for bad actors. Simply changing from using your everyday card to one of the options below will service that to varying degrees depending on your existing habits.

The second is the differences in priorities between everyone who reads this guide. Some are focused on privacy in keeping their data and information secure and to themselves. For others anonymity is more important in ensuring their actions (their purchases in this case) are open but not able to be traced back to them. Your individual priorities here will determine whether the following payment options are worthwhile investigating further.

PayPal

PayPal is basically a middleman between the buyer and the seller. As the buyer you log in to your PayPal account and process the transaction through there – you pay PayPal and PayPal pays the seller on your behalf. If using PayPal, ensure you tighten the privacy settings beyond what's standard when you open the account.

Pros	Cons
Your card information is private and not shared with the seller. Link a prepaid card for added anonymity.	PayPal needs some of your personal information to create an account
Website and app are encrypted and considered very secure	PayPal is a popular target for phishing scams
Added layer of PayPal protection with a dispute process to get your money back if your purchase turns out to be a scam	
Widespread acceptance	

Masked / virtual credit cards

Providers of these cards generate a one-time credit card number to use for purchases which means your true credit card number is never used in a transaction. So, if the seller is breached, and the bad actors recover credit card numbers yours recorded number will be worthless. This is also helpful if you must provide a credit card number for a free trial as you can set spending limits and very short-term expiry times. Companies like Privacy.com, and Abine offer these cards.

Pros	Cons
The seller doesn't get your true credit card number	The provider of the card still needs your personal information to open an account
Some providers allow you to generate cards with made-up names	The provider of the card can still see your transaction history
You can generate cards which expire after a single transaction	Typically have a $500 limit
Very secure and anonymous (anonymity not from the provider per the first con)	Cannot be used for recuring payments

Part three: Record keeping

Most people will hold on to receipts of purchases in their inbox for refund or warranty reasons. However, even in your burner email, a couple of dozen receipts reveal quite a bit about you, your interests, spending habits, and even your likely income range.

Best practise is to print the receipt and file it away in your home office or save to a secure location to avoid printing. Most importantly however **delete all emails related to the transaction** as soon as the item has arrived and appears to be working to your satisfaction.

Part four: General tips

The following are some broad tips not related to the transaction element specifically but rather safe online shopping more generally:

- Credit cards are ***typically*** **safer and have more buyer protections** in place compared to debit cards and bank transfers
- **Use a credit card from a different bank** with a small credit limit for online shopping, many people use a card linked to their savings account or the account they receive their salary. The point of this option is if the card details are breached, the damage is limited to the credit limit not the savings in the account. By using two different banks you also reduce the financial surveillance each bank can do
- **Research the reputability of the business** you are purchasing from, read their reviews, call them (turn off caller ID) and ask questions about the product, and just generally be comfortable that they're a legitimate business. Bad actors use phishing scams linking to legitimate looking websites to scam people, these are prevalent at Christmas time when people shop with urgency
- **Shop on secure websites** – these will have 'http**s**://' in the address bar with a picture of a padlock. This will protect your transaction data while in transit between your device and the seller's site
- The above point however doesn't protect your data once it reaches its destination where it needs to be protected by the seller's security protocols. Whilst these are generally quite secure, we all know breaches can happen. For this reason, it's important to **avoid the 'remember my card details for next time' option** unless necessary (such as recuring payments for subscriptions)
- **Avoid online shopping in public places** where someone can watch you over the shoulder or you can be recorded

- Most banks will offer **2FA** for purchases over a limit set by the customer. This means you will get a message on your smartphone with a code to enter before the transaction is processed
- **Never send** your bank or credit card details **by email or SMS**
- Even with your burner email, **minimise the amount** of marketing lists, newsletters, rewards / loyalty programs **you sign up for**. This also applies to participating in consumer research and satisfaction surveys.
- **Avoid coupon browser plugins** and search for deal codes manually instead

Finally, the standard good cybersecurity practises we've written about and advocate apply for online shopping as well, including:

- **Avoid financial transactions on public WiFi** (see Fake Wireless Access Point for more information)
- **Use a unique password** for each online store you purchase from
- **Be wary of phishing scams** when clicking on email offers, instead manually type in the address of the online store with the offer to validate it's legitimate
- Make sure you're **operating from a clean device** by having reputable antimalware / antivirus software in place and your software updated