Don't be phish food! Tips to avoid sharing your personal information online

May 28 2020, by Nik Thompson

Credit: William Fortunato from Pexels

Data is the new oil, and online platforms will siphon it off at any opportunity. Platforms increasingly demand our personal information in exchange for a service.

Avoiding online services altogether can limit your participation in society, so the advice to just opt out is easier said than done.

Here are some tricks you can use to avoid giving online platforms your personal information. Some ways to limit your exposure include using "alternative facts", using guest check-out options, and a burner email.

Alternative facts

While "alternative facts" is a term coined by White House press staff to describe factual inaccuracies, in this context it refers to false details supplied in place of your personal information.

This is an effective strategy to avoid giving out information online. Though platforms might insist you complete a user profile, they can do little to check if that information is correct. For example, they can check whether a phone number contains the correct amount of digits, or if an email address has a valid format, but that's about it.

When a website requests your date of birth, address, or name, consider how this information will be used and whether you're prepared to hand it over.

There's a distinction to be made between which platforms do or don't warrant using your real information. If it's an official banking or educational institute website, then it's important to be truthful.

But an online shopping, gaming, or movie review site shouldn't require the same level of disclosure, and using an alternative identity could protect you.

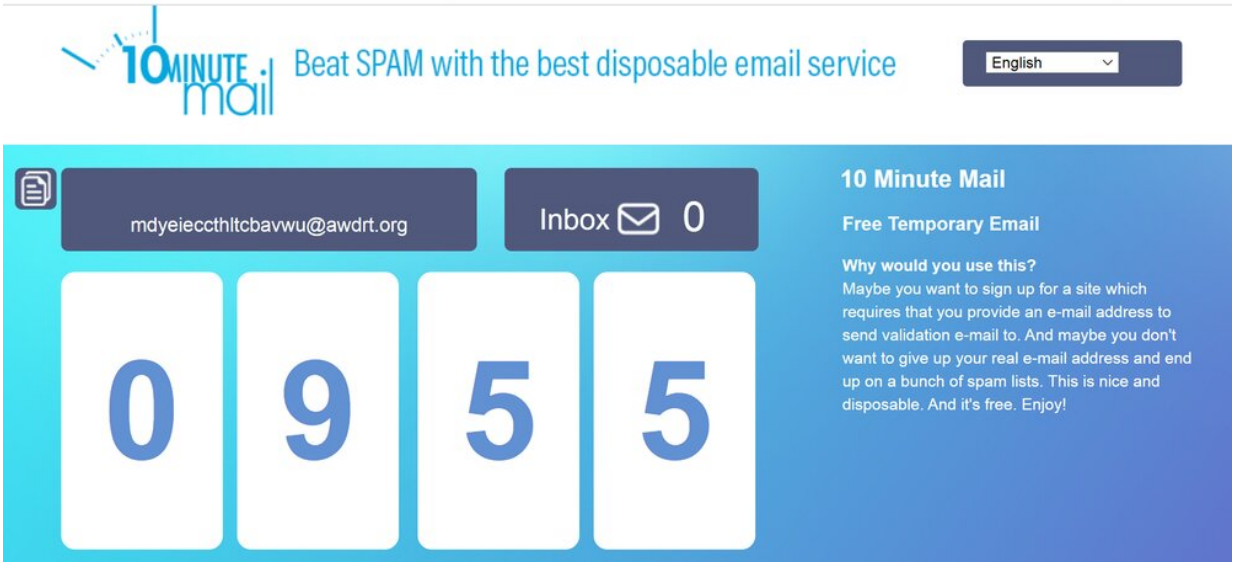
Secret shopper

Online stores and services often encourage users to set up a profile, offering convenience in exchange for information. Stores value your profile data, as it can provide them additional revenue through targeted advertising and emails.

But many websites also offer a guest checkout option to streamline the purchase process. After all, one thing as valuable as your data is your money.

So unless you're making very frequent purchases from a site, use guest checkout and skip profile creation altogether. Even without disclosing extra details, you can still track your delivery, as tracking is provided by transport companies (and not the store).

Also consider your payment options. Many credit cards and payment merchants such as PayPal provide additional buyer protection, adding another layer of separation between you and the website.



The 10 Minute Mail website offers free burner emails. screenshot

Avoid sharing your bank account details online, and instead use an intermediary such as PayPal, or a credit card, to provide additional protection.

If you use a credit card (even prepaid), then even if your details are compromised, any potential losses are limited to the card balance. Also, with credit cards this balance is effectively the bank's funds, meaning you won't be charged out of pocket for any fraudulent transactions.

Burner emails

An email address is usually the first item a site requests.

They also often require email verification when a profile is created, and that verification email is probably the only one you'll ever want to receive from the site. So rather than handing over your main email address, consider a burner email.

This is a fully functional but disposable email address that remains active for about 10 minutes. You can get one for free from online services including Maildrop, Guerilla Mail and 10 Minute Mail.

Just make sure you don't forget your password, as you won't be able to recover it once your burner email becomes inactive.

The risk of being honest

Every online profile containing your personal information is another potential target for attackers. The more profiles you make, the greater the chance of your details being breached.

A breach in one place can lead to others. Names and emails alone are sufficient for email phishing attacks. And a phish becomes more convincing (and more likely to succeed) when paired with other details such as your recent purchasing history.

Surveys indicate about half of us recycle passwords across multiple sites. While this is convenient, it means if a breach at one site reveals your password, then attackers can hack into your other accounts.

In fact, even just an email address is a valuable piece of intelligence, as emails are used as a login for many sites, and a login (unlike a password) can sometimes be impossible to change.

Obtaining your email could open the door for targeted attacks on your other accounts, such as social media accounts.

In "password spraying" attacks", cybercriminals test common passwords against many emails/usernames in hopes of landing a correct combination.

The bottom line is, the safest information is the information you never release. And practising alternatives to disclosing your true details could go a long way to limiting your data being used against you.

Provided by The Conversation