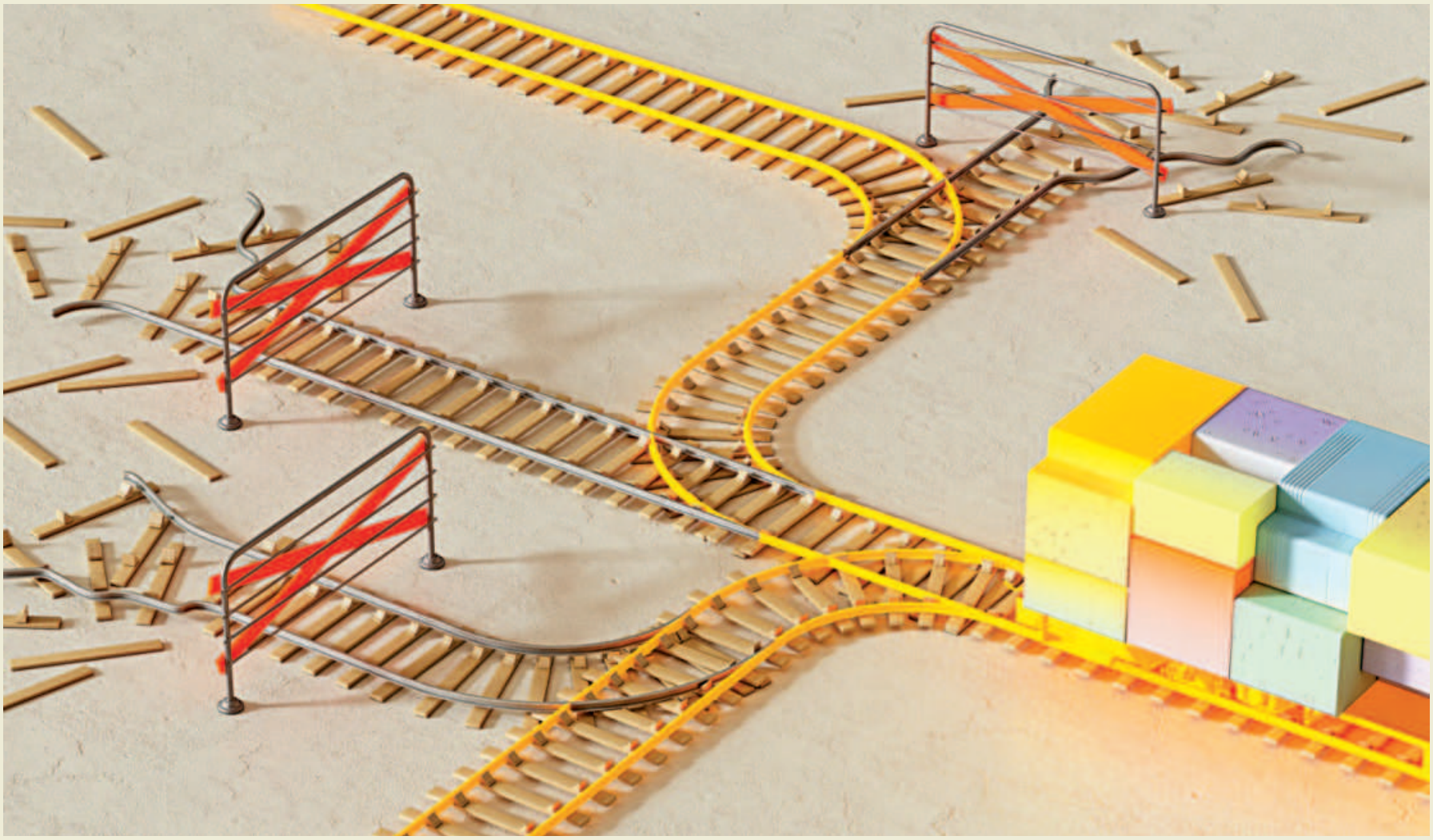

# How to keep your online information safe

In today's age of technology, a lot of our personal information is stored online, including but not limited to your home address, passport number, credit card information, and even your exact real-time location. Some websites and online services also track, collect and store your browsing habits, IP address, and what kind of devices you use - data that can be used for targeted advertising regardless of your consent. Because personal data can be stored almost anywhere on the internet, it is imperative to keep all that valuable information safe at all times. As such, here are some basic but important things to keep in mind.

**Enhance your passwords**
If you're using the same password or different variations of the same password across multiple accounts or devices, you should consider changing that; as reusing passwords tend to increase security risk for your personal information. Furthermore, having a strong password for your online profiles is the safest way to avoid a security breach. A good approach to this is to combine capital letters, numbers, and symbols such as '!' and '@' to make your password as complex as you can - while still ensuring you remember it for future use.

**Enable two-factor authentication**
Enabling two-factor authentication (2FA) on top of a strong password will make your online accounts extra secure against malicious attempts. Popular online services such as Google and Facebook have 2FA options, where you can add a second verification step that will send a unique one-time code to your mobile phone or connected device.

**Avoid phishing**
This should be obvious, but if you're a regular internet user who likes to browse a lot, be sure to avoid suspicious links in websites or emails. Normally, email services such as Gmail will filter suspicious messages as spam, but you should still keep an eye out for any phishing attempt that may go unnoticed by the AI. A good way of identifying safe websites is to look out for the padlock symbol on the address bar. This icon indicates an SSL certificate, which means the link is encrypted and will not risk exposing your information to third parties.

**Stay encrypted**
When you're browsing online, make sure you're using an encrypted link - with 'HTTPS' at the beginning of the link in the address bar. Websites with HTTPS are generally more secure and have the aforementioned padlock icon, which means your information is safe. Additionally, you can use a virtual private network (VPN) to encrypt your internet connection further. While the best VPN services are premium, if you feel your data is at risk, consider using one, especially when connected to public Wi-Fi.

**Review privacy settings**
If you use the same online account across multiple devices and haven't reviewed your privacy settings in a while, this might be a good time to do so. Be extra sure of what kind of information is being shared across your connected devices, especially social media accounts such as Facebook and Instagram which may be using your personal data to send targeted ads. Smartphone apps sometimes also require permission for your contact info, so be sure to remove such permissions from apps you feel aren't necessary.

**Keep your devices updated**
Vulnerable, outdated software always runs the risk of being hacked. Fortunately, operating systems of both smartphones and computers receive regular security updates to patch potential flaws and risks. If you want to keep your data safe, you should be on top of these updates, especially for apps that are using your personal information. You can also set your devices to install these updates automatically - though manual updates are fine too if you don't use Wi-Fi too often.

**Try adblockers**
There are plenty of adblockers and similar browser extensions available on both web and mobile browsers. You should try them out if you're worried about your data being used for targeted advertising. Not only do these adblockers not show you ads on certain sites, but they also don't allow most sites to collect your browsing data, thus improving your browsing privacy. You can also try out adblocker browsers such as Brave, Avast Secure Browser and Epic Privacy Browser.