GUIDANCE

Shopping online securely

Our wish list of security advice for online shoppers

Our advice will help you and your family enjoy a secure online shopping experience.

As well as avoiding scam websites and recognising phishing emails, these tips will help minimise any fallout should you be unlucky enough to fall victim to online crime.

1. Choosing where you shop

Seeing a padlock in the address bar is a good thing, but *it's not a guarantee that the shop itself is legitimate.* Your browser may also mark an address as "insecure" - *don't ignore this message.*

The padlock sign means that your connection is encrypted, so your personal information will reach the site without anyone else being able to read it. That's important if you're sending things like credit card details, but it doesn't tell you who is at the other end of the connection.

You need to decide whether you want to take the risk of making a purchase on a site you haven't used before. To help with this, you could do some research, for example, by checking to see if others have used the site and what their experience was.

If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases. Some other payment methods do provide good consumer protection, but they aren't obliged to provide the same protection as a credit card provider. Check their Terms and Conditions for exact details.

2. Don't give away too much information

You shouldn't need to give out your mother's maiden name, or the name of your primary school, in order to buy something. There's some obvious details that an online store will need, such as your address and your bank details, but be cautious if they ask for details that *are not required* for your purchase.

Only fill in the mandatory details of forms when making a purchase. These are usually marked with an asterisk*. If you can avoid it, **don't create an account** on a new site unless you're going to use that site a lot in the future. You can usually checkout as a guest to make your purchase.

3. Keep your devices up to date

Make sure you install the latest software and app updates. These usually contain important security updates that can protect you against identity theft.

Information can easily be found about how to install these updates from Apple, Microsoft and Google. Even better, just turn on automatic updates so your device will update itself in future.

4. Use strong passwords

Secure your important accounts with a good password - ***especially your email.*** Cyber criminals want to hack into your email account. They are looking for valuable information like bank details and the logins for your other online accounts but they'll also make use of things like your address or date of birth when trying to crack your passwords.

So, you should have a strong password for your email. One that you don't re-use anywhere else. This way, even if an attacker manages to access your email, they won't also be able to log into your online bank account.

5. Turn on two-factor authentication (2FA)

To give any online account additional protection, where possible, you should **turn on two-factor authentication (2FA).**

2FA is a way for the service you're using to double check that you really are the person you claim to be, when logging in. A common example involves the site sending a security code to your mobile phone. This ensures that any cyber criminals in possession of your password won't be able to access your account because they won't have this "second factor".

6. Use a password manager

If you have lots of accounts, the temptation to re-use passwords and usernames is pretty strong. A good way to get around this is to use a password manager.

These systems remember all your login details for you, so you can choose good passwords for each of your online accounts, without worrying about losing or forgetting them. The only password you'll need is the one for the password manager application itself. This blog post will tell you all you need to know about password managers.

7. Take care with links in emails and texts

Once you start shopping, stay alert. Some of the emails or texts you receive about amazing offers may contain links to fake websites, designed to steal your money and personal details.

Not all links are bad, but if you are unsure don't use the link, go separately to the website.

8. When things go wrong

We all make mistakes and these days the scams can be incredibly convincing.

If you think you may have been taken in by a bogus website, you should first, take a note of the website's address, then close down your internet browser. Then report the details to Action Fraud and contact your bank to seek advice.

Whether you've been a victim of fraud will depend on how much information you've provided to the website. So keep an eye on bank transactions, if you can. Contact your bank immediately about anything that you don't recognise, even small amounts.

PUBLISHED

17 January 2019

REVIEWED

20 April 2020

VERSION

1.0

WRITTEN FOR

Individuals & families