ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is not an emergency service
dial 999 if you are in immediate danger.

Keep hackers out of your email and social media accounts

If a hacker got into your email or social media account, what would they find? Health and banking information? Names and contact details for your friends and family? Private photos and messages? For most people, it's at least one of those.

Your email and social media accounts contain a wealth of personal information about you, which makes them a lucrative target for cyber criminals. Between February 2020 and February 2021, Action Fraud received 15,214 reports about email and social media account hacking. The majority of reports (88%) were made by individuals, with 12% of reports being made by businesses.

Analysis of the crime reports revealed that Facebook, Instagram and Snapchat were the most affected social media accounts, with phishing messages being the most common tactic used by cyber criminals to lure unsuspecting victims.

The motivation behind the hacks are varied and can range from financial gain, to revenge or personal amusement. Some victims are extorted for money, whilst others have their accounts used to send malicious links to their contacts. One victim who had multiple email and social media accounts hacked paid over £2,000 to regain access to them. Another victim reported that her hacked Facebook account was used to trick her friends into sending money into a PayPal account they thought belonged to her.

Superintendent Sanjay Andersen, Head of the City of London Police's National Fraud Intelligence Bureau, said:

"Criminals hack people's email and social media accounts to access a wealth of valuable personal information about the individual, which they can use to commit fraud. This includes passwords for other accounts like online banking. Criminals also use compromised accounts to imitate the victim online and trick their family and friends into sending money.

"One of the most important things that you can do to improve the security of your online accounts is having two-factor authentication enabled. Not only will it prevent hackers accessing your accounts even if they have your password, but it will also keep your valuable information out of the hands of criminals."

How to keep hackers out of your email and social media accounts

1: Secure your email accounts

If a hacker gets into your email, they could:

- reset your other account passwords
- access private information such as contacts, messages or photos.

Your email password should be strong and different to all your other passwords. This will make it harder to crack or guess. Using 3 random words is a good way to create a strong, unique password that you will remember. Enable Two-factor authentication (2FA) in your email account settings, it will help to stop hackers from getting into your account, even if they have your password.

How to change your email password:

- Gmail (opens in a new tab)
- Yahoo! Mail (opens in a new tab)
- Outlook (opens in a new tab)
- BT (opens in a new tab)
- AOL Mail (opens in a new tab)

2: Enable two-factor authentication (2FA)

If a hacker gets into your social media account, they could:

- access private information such as contacts, messages or photos.
- send messages containing malicious links to your followers.
- trick friends or followers into sending them money by pretending to be you.
- extort you for money in exchange for restoring access to your account.

Use three random words to create a strong, unique password for your social media accounts. Enable Two-factor authentication (2FA) in your account settings, it helps to stop hackers from getting into your accounts, even if they have your password.

How to turn on two-factor authentication (2FA)

For email accounts:

- [Gmail (opens in a new tab)](#)
- [Yahoo (opens in a new tab)](#)
- [Outlook (opens in a new tab)](#)
- [AOL (opens in a new tab)](#)

For social media accounts:

- [Instagram (opens in a new tab)](#)
- [Facebook (opens in a new tab)](#)
- [Twitter (opens in a new tab)](#)
- [LinkedIn (opens in a new tab)](#)

Watch out for suspicious messages

Be cautious of social media messages that ask for your login details or authentication codes, even if the message appears to be from someone you know.

What to do if one of your online accounts has been hacked

If your email or social media account has been hacked, it's important that you act fast. Here's some [useful information](#) on the steps you can take to try and recover the account.

Report it

If one of your online accounts has been hacked, report it to Action Fraud by visiting www.actionfraud.police.uk, or calling 0300 123 2040.