CYBER AWARE

south east
Regional Organised Crime Unit

E-Mail Compromise

Surrey & Sussex CCU Newsletter – October 2020

If you are online, your electronic mail or e-mail account is probably one of the most important aspects of your cyber activity. Many of us have had the same e-mail address for decades and it has almost become part of our identity. Of course, you will use your e-mail address to communicate with friends and business associates, but you will also use it as your username for numerous different online accounts, a way to recover lost credentials, proof of identity and a bunch of other things. Nowadays, e-mail addresses can be the portal to your entire online existence – think about Microsoft 365 and how this allows access to both personal and business platforms. As a result, a compromised e-mail address can be extremely distressing and can often lead to huge problems including identity theft, mandate fraud and an almost total loss of online control.

Microsoft 365

What is a compromised e-mail account?

Your e-mail account becomes compromised when someone gains access to it without your permission. And, if you haven't taken some basic security precautions, it's pretty easy to do.

Your e-mail address is a little like your physical address. It's easy to find out if it exists, but you need the key to get in (i.e. a password). Criminals are adept at getting passwords. They can get them from phishing – cleverly crafted e-mails or text messages designed to trick you into providing your credentials. They can get them from data breaches where username and password combinations are offered for sale. If your password is weak, they can brute force it by trying hundreds or thousands of different passwords. They can even get passwords from Post-It notes left near your computer, guessing them or by watching you typing it in on the train or bus.

What happens next?

amazon

It depends on what they find and what they want to do. Sometimes, criminals will change the security settings to prevent you from accessing the account – leaving them with total access to your e-mails and online content. They may use your e-mail to ask your contacts for money. They will inevitably try and get access to other online accounts (such as social media or shopping sites) that are accessed with your e-mail address. Most people keep e-mails for a long time – so criminals will be able to obtain extensive personal information about your history which could be used for identity theft, blackmail or other malicious purposes.

Depending on the type of e-mail account that gets compromised, criminals may not want to advertise that they have managed to access the account.

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk

CYBER AWARE

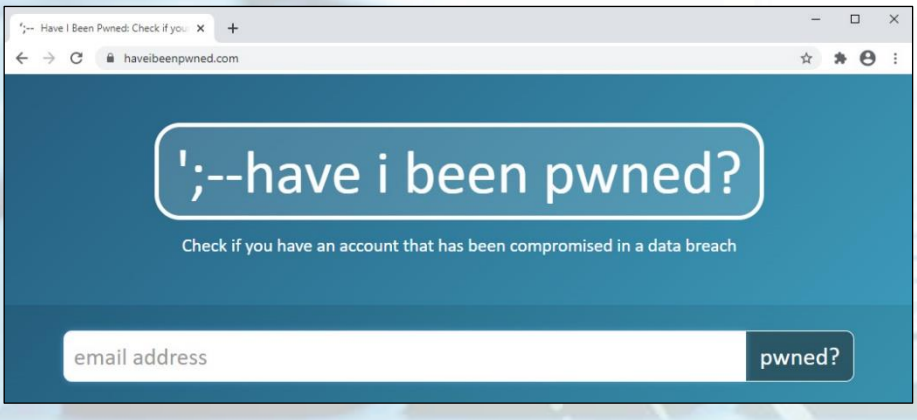
south east
Regional Organised Crime Unit

Mandate Fraud

Mandate fraud takes place when a criminal manages to change banking details meaning that payments are made to the wrong account. It is easy to determine if a compromised e-mail account is used for financial activity as there will generally be a history of payments on the account. Criminals will often make use of e-mail rules to ensure they can read all e-mail before the intended recipient. In the event of a significant payment, they will intercept the e-mail, change the banking details on the invoice and then drop it back in the inbox for the intended recipient. Without additional security checks, the payment will then be made to the criminal's account.

What can I do to prevent this?

- Protect your account with a strong password. Remember, a strong password will consist of at least 3 random words, be longer than 12 characters and include numbers, symbols and capital letters. It will be unique to that account and not used for other accounts.
- Use 2-factor-authentication(2FA). This is sometimes called 2-factor verification and is an additional layer of security to prevent criminals accessing your account. Visit www.telesign.com/turnon2fa for more information on 2FA.
- Businesses should consider the way they manage payment requests received by e-mail to mitigate the risk of mandate fraud.
- Check your e-mail rules regularly to ensure you are the author of them.
- Check your account security history to ensure no unusual login activity is taking place.
- Check for compromised accounts at https://haveibeenpwned.com/ . Remember to change any that have been compromised and register to receive notification of future data breaches involving your username(s).



Who do I report this to?

Action Fraud is the first port of call for any cyber-crime reporting. You can visit the Action Fraud website at https://www.actionfraud.police.uk/. You will need to create an account, but this can then be used for any subsequent reports.

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk