Extortion scam

Cyber criminals send victims their own passwords in extortion scam

Cyber criminals are attempting to blackmail unsuspecting victims by claiming to have used their password to install spying malware on their computer. The criminals claim they've recorded videos of the victim watching adult material by activating their webcam when they visit these websites. What makes this scam so convincing is that the email usually includes a genuine password the victim has used for one of their online accounts. We believe criminals obtain the passwords from data breaches.

What to do if you get one of these emails?

Don't reply to the email, or be pressured into paying. The police advise that you do not pay criminals. Try flagging the email as spam/junk if you receive it multiple times. Perform password resets as soon as possible on any accounts where you've used the password mentioned in the email. Always use a strong, separate password for important accounts, such as your email. Where available, enable two-factor authentication (2FA). Always install the latest software and app updates. Install, or enable, anti-virus software on your laptops and computers and keep it updated.

If you receive one of these emails, report it to Action Fraud's phishing reporting tool. If you have received one of these emails and paid the ransom, report it to your local police force.