7 MEASURES TO TAKE WHEN A SEXTORTION SCAM LANDS IN YOUR MAILBOX

A guide for employees

1. Act slowly and deliberately, and avoid rash steps.

Criminals behind sextortion scams target human weaknesses and try to manipulate you into harmful action. Therefore, if you receive a fear-inducing message, stop and consider the possibility that nothing in the email is true. If you are unsure, always consult the IT department or tech support of the security provider.

2. Don't pay the (s)extortionists.

Sextortion emails are usually just scams. This means there is no merit behind the claims of the criminals, they almost certainly have no video of you or what you watched, they are not with law enforcement, and they didn't order a "hit on you." By paying the demanded sum, you only lose money and fuel the business of criminals, helping them to spread more scams.

3. Do not interact with the email in any way.

Do not reply to the scam, do not download its attachments, do not click on embedded links or interact with any of the contents, as these elements can lead to malware or other threats.

4. Send the email to your IT department.

Some companies consider spam and scams as security incidents. If that is the case, the user is obligated to notify their IT department or internal security. In smaller companies, where IT security is provided by a third party (e.g. MSP), employees are advised to contact the security provider and ask for further instructions. If your company has no IT staff, the least you can do is to scan the computer and network with a reliable security solution and make sure that any of your passwords haven't been leaked or compromised.

5. Check/change your password.

In some cases criminals test the leaked credentials and if successful, use the hacked account at least to spread their messages. Therefore, if an attacker lists any of your actual passwords, change them immediately and activate multi-factor authentication to increase their protection.

6. Secure your web cam.

To avoid possible misuse of the built-in webcam, use protective software or at least put a piece of tape over the camera. This way, you can be certain that criminals have no way to record a video of you sitting in front of the device.

7. Use an anti-spam solution.

A reliable security solution with anti-spam functionality can also help stop sextortion scams from landing in the inbox in the future.

ESET