Information sent on behalf of Action Fraud (National Fraud Intelligence Bureau)

Law Abiding Citizen Alert

Fraudsters are sending out a high volume of phishing emails to personal and business email addresses, pretending to come from various email addresses, which have been compromised.

The subject line contains the recipient's name, and the main body of text is as below:

"Hi, [name]!

I am disturbing you for a very serious reason. Although we are not familiar, but I have significant amount of individual info concerning you. The thing is that, most likely mistakenly, the data of your account has been emailed to me.

For instance, your address is:

[real home address]

I am a law-abiding citizen, so I decided to personal data may have been hacked. I attached the file – [surname].dot that I received, that you could explore what info has become obtainable for scammers. File password is – 2811

Best Wishes,"

The emails include an attachment – a '.dot' file usually titled with the recipient's name.

This attachment is thought to contain the Banking Trojan Ursniff/Gozi, hidden within an image in the document. The Ursniff Banking Trojan attempts to obtain sensitive data from victims, such as banking credentials and passwords. The data is subsequently used by criminals for monetary gain.

Protect Yourself:

Having up-to-date virus protection is essential; however it will not always prevent your device(s) from becoming infected.

Please consider the following actions:

Don't click on links or open any attachments you receive in unsolicited emails or SMS messages: Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication (you can find out how by searching the internet for relevant advice for your email provider).

Do not enable macros in downloads; enabling macros will allow Trojan/malware to be installed onto your device.
Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It is important that the device you back up to is not connected to your computer as any malware infection could spread to that as well.
If you think your bank details have been compromised, you should contact your bank immediately.

If you have been affected by this or any other fraud, report it to Action Fraud by calling 0300 123 2040, or visit www.actionfraud.police.uk.

Message sent by
Action Fraud (Action Fraud, Administrator, National)