Dear Marianne,

We understand that the situation is serious but please remain calm.

I have been working on the incident (with the help of the information provided to me from Fatima Osei) to get to the root cause of the incident. Chances are that the attacker has access to your login credentials which means that the cyber-attacker can gain unauthorised access to confidential information.

I would recommend you familiarise yourself with phishing attacks. I have contacted the Incident response team to recommend setting up an employee training programme in phishing attacks to prevent this situation from happening in the future. It is important to keep up to date with phishing attacks and to distinguish a real email from a malicious email.

By using the information that has been given to me to help investigate this further you will know whether the security measures I have suggested will be made in due course regarding phishing emails so to prevent this incident from happening again.

You should reset your password as soon as possible.

Jose from level 1 security team provided the most up-to-date legitimate link for you to reset your password.

Please copy and paste this hyperlink into your web browser:

https://accounts.steeldoordata-oc.com/passwordreset

Make sure to also delete the phishing email to prevent accidentally clicking on it.

Yours sincerely,

Darius Richardson
Junior analyst

Dear Alex,

I have taken serious action on addressing the severity and impact of the incident as well as providing solutions and security measures to put in place to recover any potential data loss and prevent this situation from happening in the future.

The invoice that you downloaded is what caused the malware to affect your computer causing it to not work and possibly cause the malware to spread to other systems because of your callous action.

To inform you, we will do a factory reset to delete everything from the computer including windows and then install everything.

I also propose that an employee training programme is taking for all employees to identify what a malicious email looks like to prevent this from happening again.

Make sure to delete the email with the attachment to prevent accidentally clicking on it.

Yours sincerely,
Darius Richardson
Junior Analysis