Dear Marianne,

Thank you for reporting the issue with your account. After investigating, we've determined that the problem occurred because of a phishing email you received, which led you to enter your account credentials on a fraudulent website.

We understand how convincing these emails can look, but entering your credentials on an unverified website has serious implications. This incident resulted in the compromise of your account, and if not addressed quickly, could have led to unauthorized access to sensitive business information.

This kind of mistake, while unintentional, could have significant consequences for the company, including financial losses or legal risks. It is important to be vigilant when responding to emails, especially those requesting sensitive information.

What You Should Do Moving Forward:

1. Always verify the legitimacy of emails by checking the sender's address and any links provided.
2. Use only trusted, official channels for password resets or other account-related actions.
3. Complete the attached phishing awareness training to better identify and avoid fraudulent attempts in the future.

Your cooperation in learning from this situation is crucial to protecting our organization. If such incidents are repeated, they could lead to formal corrective actions.

We've taken steps to secure your account and prevent further unauthorized access. Please follow the link below to reset your password immediately using our official site:
https://accounts.steeldoordata-oc.com/passwordreset

Thank you for your understanding, and please let us know if you have any questions.

Best regards,

Luis Cruz
Steel Door Data Protection - Security Team

Dear Alex,

Thank you for reporting the issue with the email and attachment you received. After investigating, we've confirmed that the attachment you opened contained malicious software. This file attempted to run harmful commands on your computer, which could have allowed attackers to gain further access to our network.

While the issue was contained and no additional damage occurred, opening unverified email attachments poses a significant risk to the company. It could lead to the compromise of sensitive business information, loss of customer trust, and even legal repercussions. Such actions could also result in formal corrective measures if repeated.

What You Should Do Moving Forward:

1. Never open email attachments from unknown or untrusted senders, especially if the email seems urgent or suspicious.
2. Verify the legitimacy of emails with the IT team before taking action.
3. Complete the attached training module to better identify potentially harmful emails and attachments.

To ensure there are no lingering risks, we will be reimaging your computer. This process will erase all files and settings and reinstall the operating system. Please back up any critical files you need immediately.

Your cooperation is essential to maintaining a secure working environment. If you have any questions about this process or need assistance, don't hesitate to reach out.

Best regards,

Luis Cruz
Steel Door Data Protection - Security Team