Office 365 Compromised Account / Password

If you think that your Office 365 account has been compromised then there are a few simple thing that you can do.

This is what Microsoft recommends:

The Problem

You have issues when you when you try to sign in to Microsoft Office 365. Or, you notice that suspicious activity occurs in your account, such as large amounts of spam that originates from your account.

You may also experience one or more of the following issues:

- The Sent or Deleted Items folders in Microsoft Outlook or in Microsoft Outlook Web App contain common hacked-account messages, such as "I'm stuck in London, send money."
- Unusual profile changes, such as the name, the telephone number, or the postal code were updated.
- Unusual credential changes, such as multiple password changes are required.
- Mail forwarding was recently added.
- An unusual signature was recently added, such as a fake banking signature or a prescription drug signature.

Solution

Even after you've regained access to your account, the attacker may have added back-door entries that enable the attacker to resume control of the account.

To help resolve these issues, you must perform all the following steps within five minutes of regaining access to your account to make sure that the hijacker doesn't resume control your account. These steps help you remove any back-door entries that the hijacker may have added to your account. After you perform these steps, we recommend that you run a virus scan to make sure that your computer isn't compromised.

Step 1:

Make sure that your computer isn't compromised

1. Make sure that you have Windows Update turned on.
2. If antivirus software isn't installed on your computer, we recommend that you install antivirus software and then run a scan to make sure that no malicious software is installed on the computer. You can download free anti-malware or antivirus software from Microsoft.

Step 2:

Make sure that the attacker can't log on to your Office 365 account

1. Change your password immediately. Make sure that the password is strong and that it contains upper and lowercase letters, at least one number, and at least one special character.
2. Don't reuse any of your last five passwords. Even though the password history requirement lets you reuse a more recent password, you should select something that the attacker can't guess.
3. If your on-premises identity is federated with Office 365, you must change your password on-premises, and then you must notify your administrator of the compromise.

Step 3:

Make sure that the attacker can't resume access to your account

1. Make sure that the Exchange account doesn't auto-forward addresses.
2. Make sure that the Exchange server isn't sending auto-replies.
3. Make sure that your contact information, such as telephone numbers and addresses, is correct.

Step 4:
Additional precautionary steps

1. Make sure that you verify your sent items. You may have to inform people on your contacts list that your account was compromised. The attacker may have asked them for money, spoofing, for example, that you were stranded in a different country and needed money, or the attacker may send them a virus to also hijack their computers.
2. Any other service that used this Exchange account as its alternative email account may have been compromised. First, perform these steps for your Office 365 subscription, and then perform these steps for your other accounts.

For more information call us on 02476 998229.