Scramble Corp

ADDITIONAL SECURITY MEASURES

Date: 04/09/2021
FAO: All employees
Author: IT Support

As you may have heard, our network was recently compromised and an attacker was able to access all of our data. We have identified the way the attacker was able to gain access and have made some immediate changes. You can find these listed below along with the ways these changes may impact you.

Change: As the attacker used something known as "NTLM relaying", we have disabled NTLM authentication across the entire network.

Users impacted: All

Workaround: When you log on or access network resources you will now be using Kerberos authentication (*which is definitely 100% secure and has absolutely no way anyone could exploit it*). This will require you to use the full domain name (scrm.local) with your username and any server names you access.

Change: The attacker was able to retrieve credentials from an SQL database used by our HR software so we have removed all access to the SQL service for everyone apart from network administrators.

Users impacted: HR department

Workaround: If you can no longer access the HR software please contact us and we will manually grant your account access again.