BLACKCLOAK®

CEO Takes Back Control of Personal Privacy from Rogue IT

Description

- CEO of retail company
- Married with and two children
- Multiple homes
- Sophisticated home automation and wireless network in each home

The Problem

The CEO's retail company employed an IT professional who crossed the line of their responsibilities by taking control of the CEO's home network, personal device security and the family's emails from the office.

Taking back control proved harder than expected as the IT professional refused to provide the CEO with the passwords needed to control her home wireless network. She was also concerned that the IT professional would retaliate against her family or the company, but needed to ensure that she and her family were secure from the intrusion.

The final straw came when the IT professional pranked the CEO and her family on their home computers. The CEO needed to protect her family and the company, but needed guidance to do so securely.

BlackCloak Steps In

The CEO needed the support of cybersecurity professionals outside the organization in order to bring order back to her company and personal digital life. She reached out to BlackCloak and replaced the IT professional immediately with a new, outsourced IT provider recommended by BlackCloak. The new provider began by replacing all existing physical devices.

Once done, BlackCloak was able to secure the CEO's homes and personal infrastructure. Working together, BlackCloak and the new IT provider tightened up family privacy by reducing the family's online presence through data broker removal services, hardening personal device security and installing security monitoring software, and placing personal privacy protections on all accounts, and adding deception technology to all devices for advanced tracking of hacking attempts.

BlackCloak's comprehensive personal privacy protection plan continuously and proactively protects the family's devices and homes.

Our Four-Step Plan:

01.

Harden the account. We kicked out unauthorized devices and apps that had access to her mail account. We also changed her password and enabled multi-factor authentication (MFA), further blocking the threat actor's access.

02.

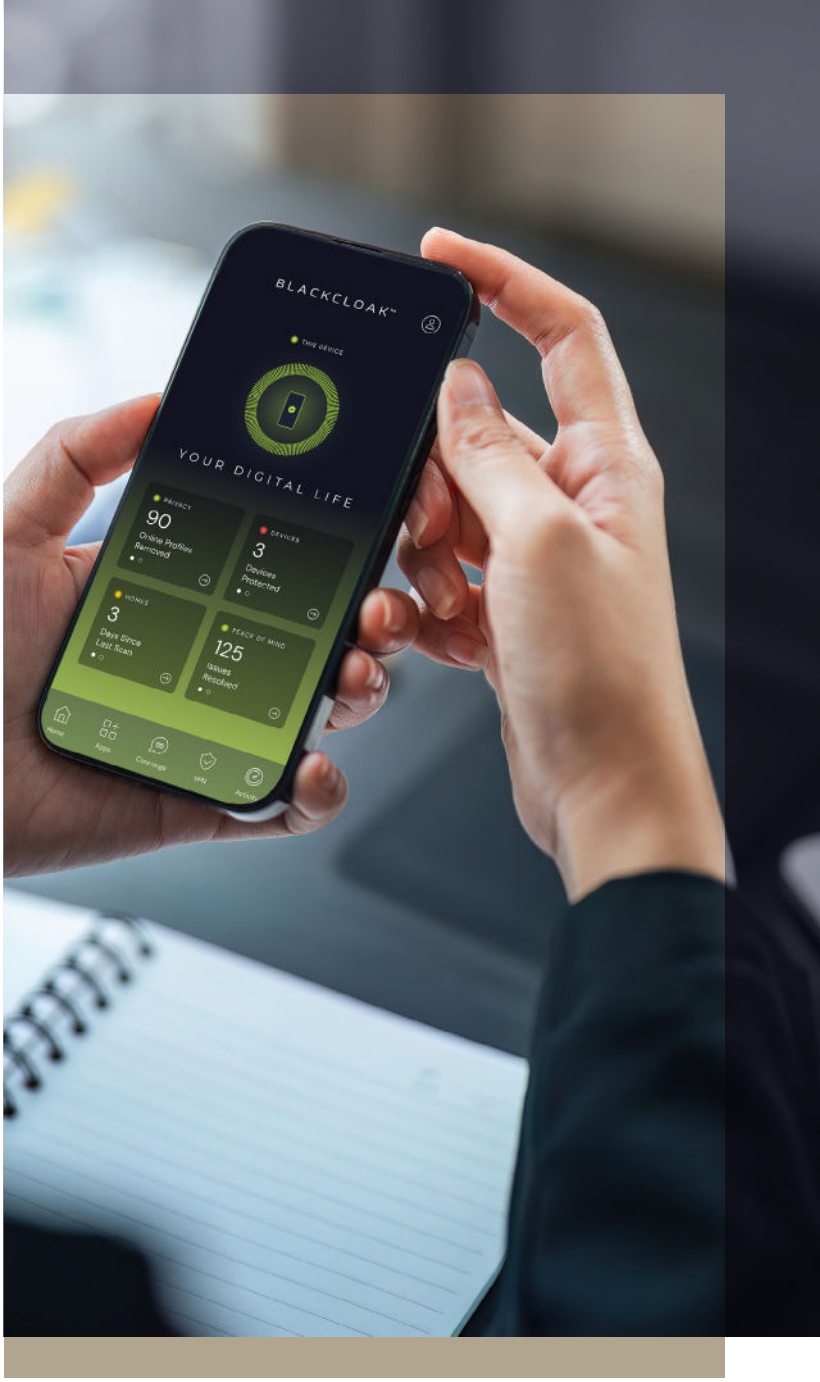
Changed account permissions. The threat actor used other platforms like Thunderbird, BH Mailer, and Email by Edison to log into her email. We blocked permissions from such external sites and platforms to prevent future malicious activity.

03.

Identified other "pivot points" accessed by the bad actor: The threat actor had gained access to several other personal accounts, even booking a flight using her loyalty points. We changed all passwords and initiated mult-factor authentication on such accounts. We set her up with a password manager to ensure her account logins were secure.

04.

Began ongoing identity monitoring: We searched the dark web and minimized her digital footprint from data broker sites to ensure her identity was not for sale and could not be further compromised.



The Result

In reaching out to BlackCloak, the CEO and her family successfully prevented the former company IT professional from accessing their life, home, network, and personal computers. This protected the company and the entire family from data loss, extortion, and negative business impact. They now have a secure wireless network and home automation system, have privacy for their entire family, and have a trusted concierge team in place for all future questions and issues.