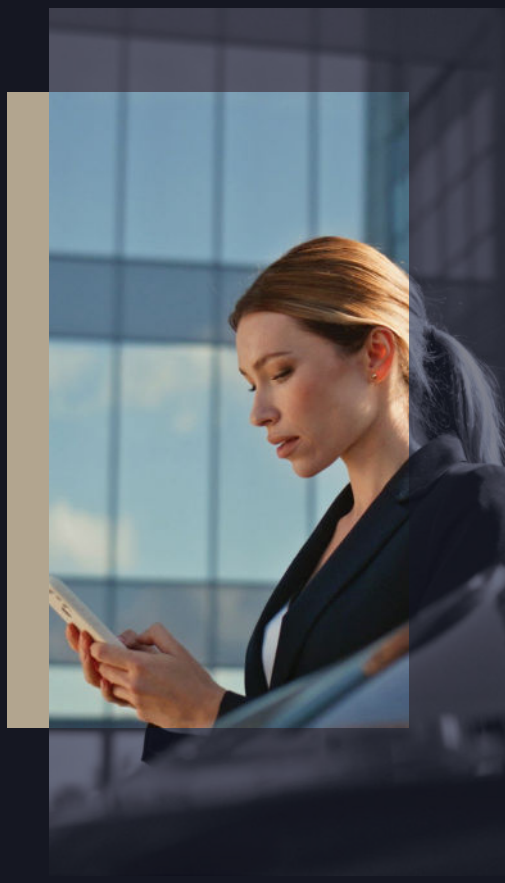
BLACKCLOAK®

Private Client Secures Email, Follows Good Cyber Hygiene to Stop Future Attacks



A Client Success Story

The warning signs were there. A compromised email account led to other personal exposures for this member.

- Numerous suspicious email drafts containing threatening messages from a malicious hacker.
- Rogue Apple Pay charges.
- Unrecognized outgoing emails from her email account.

The Problem

Our private client discovered dubious activity in her Hotmail account, indicating that her personal email had been compromised by a malicious threat actor. Her employer also notified her that her bank had contacted them requesting a direct deposit, which appeared suspect.

She needed help from the experts. She called on BlackCloak.

BlackCloak's Guidance

Our Security Operations team investigated her email account and immediately discovered a few telltale signs: drafts containing "ransom" messages addressed to the client, and several thousand emails sent to unrecognized recipients from her email. Additionally, the threat actor had created a rule that forwarded all of her received emails – including security alerts and password reset messages – into her spam folder, ensuring that the hacker would remain undetected.

BlackCloak discovered that numerous other personal accounts were also compromised, such as her Apple Pay, Costco, Venmo, and United Airlines accounts, among others. Once accessing and lurking in her email for a period of time, the hacker had gained access to these accounts, changed her passwords, and attempted to commit fraud.

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.

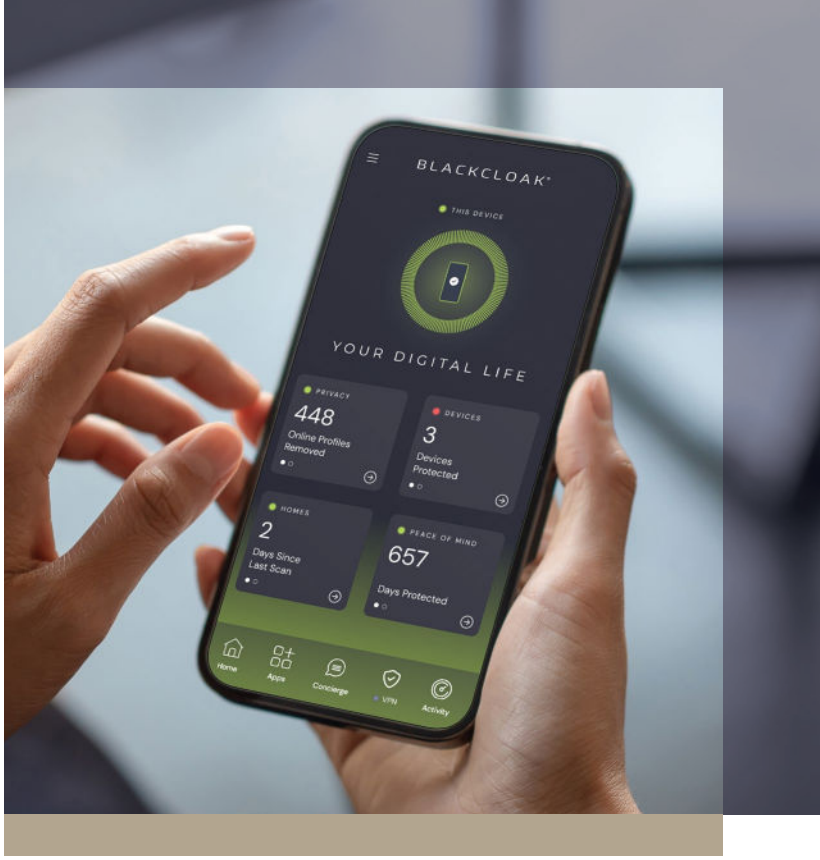
Changed account permissions. The threat actor used other platforms like Thunderbird, BH Mailer, and Email by Edison to log into her email. We blocked permissions from such external sites and platforms to prevent future malicious activity.

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

Once the BlackCloak team secured our client's email account and digital footprint, we conducted a workshop to teach her about cybersecurity hygiene best practices. We also set up MFA on all her personal accounts and moved her to an external password manager to protect and manage her login credentials.

On an ongoing basis, we keep her personal devices protected through the BlackCloak endpoint detection and response (EDR) and anti-malware solution, which detects malicious files and is monitored by the Security Operations Center (SOC) 24/7. The BlackCloak Security Operations Center (SOC) is also available to help assess the validity of emails she receives. We provide ongoing identity monitoring and conduct periodic digital footprint assessments to give her peace of mind that she will not fall victim to another malicious scam.

This is just one of many examples demonstrating BlackCloak's unwavering commitment to providing our customers with trusted, superior Digital Executive Protection and highlights the effectiveness of our holistic approach to cybersecurity.