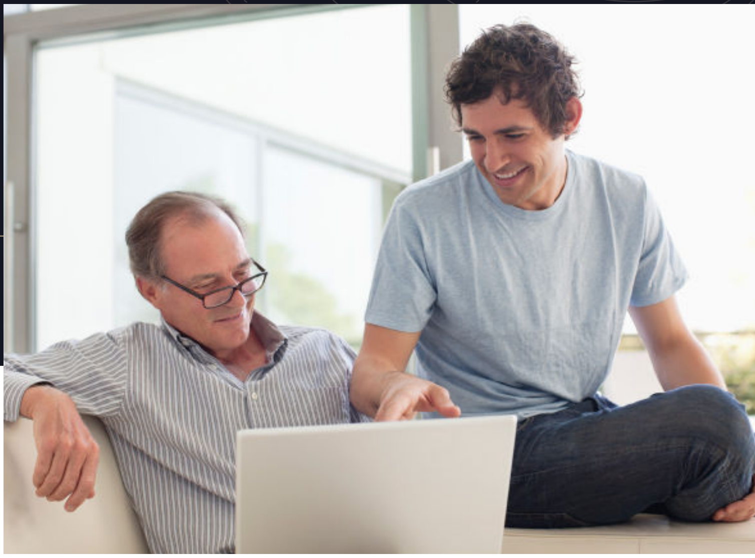
BLACKCLOAK™

Reclaiming Digital Identities: Overcoming Ransomware and Account Takeovers

Client Profile

Mark: Son, small business owner*
Allen: Father, partial business ownership*



The Challenge

Mark is in his 20s and owns his own gym as well as a personal training business. He was having great success with a maximum amount of gym members and a regular roster of clients. To support his business, he has a website that is hosted through a popular platform provider and used a calendar application to allow his client to book appointments with him.

As his business became more successful, Mark had less time to maintain the day-to-day maintenance of his website so he began a search for someone to manage it on his behalf. He turned to a well-known platform to source freelancers that provide the services he needed. He quickly found someone who could help him and they began working together.

Shortly thereafter, Mark's world changed as his new website manager turned out to be a cybercriminal. Very quickly, using social engineering techniques (a tactic used by cybercriminals to trick people into revealing sensitive information or performing actions that compromise their security), the threat actor remotely connected to Mark's Microsoft Windows computer.

This access point allowed the attacker to infiltrate Mark's Google Gmail, Apple iCloud, Microsoft Office 365, Facebook, and Instagram accounts, as well as take over Mark's business domain and calendaring application. The threat actor even began impersonating Mark, reaching out to family members, requesting money.

Additionally, the threat actor infected the computer with ransomware and also was able to access Mark's father's accounts. The severity of the compromise posed significant risks, including potential network takeover and further breaches.

Mark and his father, Allen, were unable to access their own accounts. Mark was losing significant business as his existing clients could not book time with him, nor could he advertise his services on Facebook (his primary marketing platform) to obtain new clients.

The Solution

Allen knew he had to act quickly, both to gain back access to his own accounts and prevent Mark from continuing to lose income. After some research and speaking with colleagues, he reached out to BlackCloak for immediate assistance.

The BlackCloak team jumped into action, initiating an emergency onboarding session.A member of the **BlackCloak Cyber Security Operations Center *(CSOC)*** team made an in-person visit to Mark's home and began to remediate the situation.
The team member conducted an internal network scan and vulnerability testing to identify and assess the extent of the compromise.

To begin remediation, the BlackCloak team member wiped the computer to get rid of the ransomware, ensuring that any unauthorized access was terminated.

They then set about regaining access to existing accounts. Because there were so many accounts to save, the team prioritized the ones that had a direct effect on Mark's livelihood. They were able to get back into Mark's Gmail account, the website domain, and the calendaring service first. They then focused on each of the other accounts, and after nearly 15 hours of work, were able to access all of Mark's and his father's accounts that were compromised.

All passwords were reset and accounts hardened. By establishing a robust security baseline, BlackCloak ensured that any future threats could be swiftly identified and remediated. **Each of Mark and Allen's individual devices were onboarded to the BlackCloak Concierge Cybersecurity & Privacy™ Platform to ensure constant monitoring.**

Results

After the BlackCloak team had secured Mark and Allen's respective digital footprints, coaching and training on cybersecurity hygiene was initiated to ensure that they both knew how to identify cyber threats in the future. This comprehensive approach provided Mark and Allen with the confidence and peace of mind that their digital assets were secure.

Through swift and decisive action, Mark and Allen were able to mitigate the immediate threat, recover compromised accounts, and fortify the digital defenses with the help of BlackCloak. This case study underscores BlackCloak's commitment to providing exceptional digital executive protection and highlights the effectiveness of our holistic approach to cybersecurity.

**All names (and specific details) have been changed to protect the client's privacy.*