CYBER EXPOSURE HITS TOO CLOSE TO HOME FOR ONE FINANCIAL INSTITUTION CEO

The CEO of a major U.S. financial institution engaged BlackCloak provide cybersecurity protection to his entire family. The family is often in the public eye, travels abroad frequently, and has various household personnel that share the family's home network.

During its review of the children's' computers, BlackCloak identified over 140 instances of malware on one device alone. The malware included fake antivirus, potentially unwanted programs (PUPs), adware, and other keyboard logging software. Keylogger software is particularly dangerous, in that it captures and logs what a user types on the keyboard--typically without the user knowing. With this tool, a cybercriminal has the ability to determine passwords entered, websites visited, and emails sent, among other things. The client had always worried about the internet safety of his children, and this discovery hit very close to home. It was especially unnerving, given the potential for private family--and even business--communications to be exposed to unauthorized individuals and hackers.

BlackCloak ensured proper eradication of the malware from the infected computer, scanned the home network for other threats, and left the children and family with a safe computing environment.

The client now has BlackCloak protecting not only his family, but also key household personnel, as well as the 10 other executives at the financial institution. The client was not willing to risk the executive team having a personal cyber incident that might impact the business operations of the financial institution.

© 2019 BLACKCLOAK. All rights reserved.
CONFIDENTIAL