BLACKCLOAK®

Watch Out for These Cyber Scams Targeting HNW Families and Executives

Phishing attacks are one of the most common cyberattacks in the digital ecosystem.

Phishing is considered a social engineering attack where one party uses deceptive tactics, such as posing as a legitimate entity, to manipulate their targets into turning over sensitive information or enticing them to take a specific action, often by sending them an email with urgent, time-based next steps.

Our cybersecurity and privacy partner, BlackCloak, shared the most common scams that specifically target executives, board members, and high-profile persons directly.

Swatting and Doxxing

- Cybercriminals are using information from the dark web (which cannot be erased), data broker information (which BlackCloak removes regularly), and property record information to target you. These records can have your name and address on them. This type of activity is referred to as "Doxxing."

- With this information, cybercriminals are calling (using spoofing technology) your local police department to report a hostage situation or heinous crime in progress and giving them your address. Law enforcement officers are required to respond to this call and in many cases, SWAT teams are dispatched to your home. This type of activity is called "Swatting."

Refund Payment Portal Impersonators

- The FBI issued a warning about cybercriminals impersonating financial institutions. Potential victims are sent an email where they are told to cancel a subscription within 24 hours or they will be charged a $300 to $500 penalty. The email includes a phone number where victims are told a representative can help them cancel the service and get a refund. When a target calls the number, the scammer will persuade them to give control of their devices as well as credentials for their bank accounts. Doing so can either lock the target out of their devices, or black out the screen while they conduct a wire transfer.

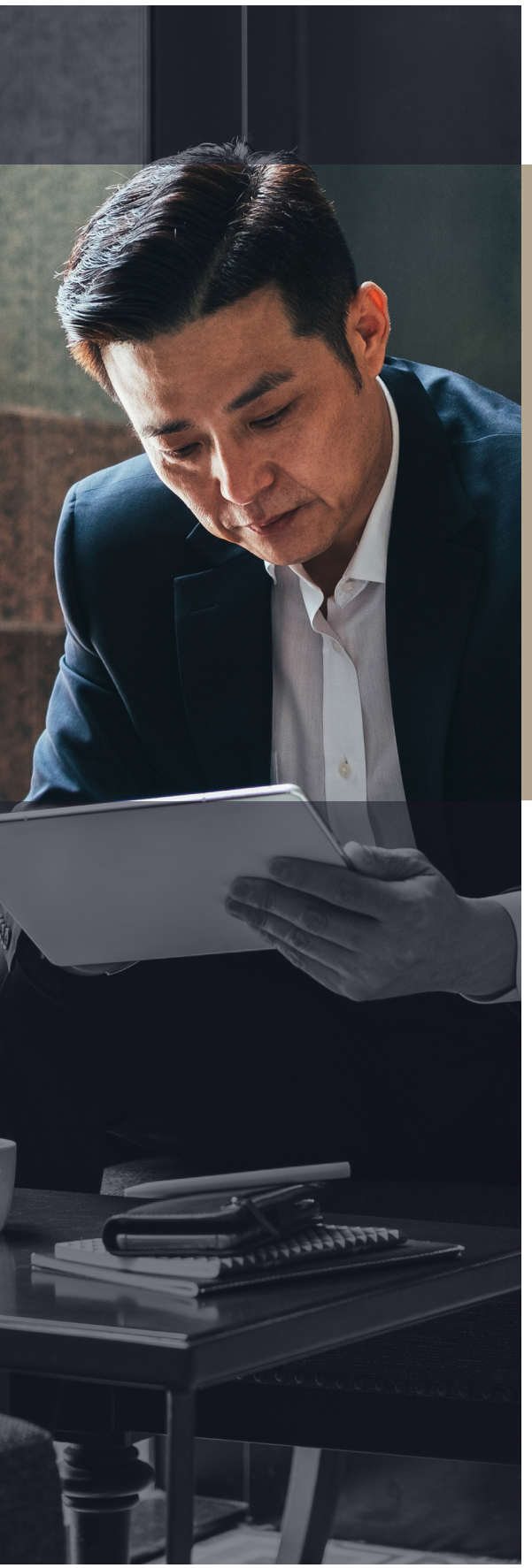


Image-Based Phishing Scams

- Scammers can create phishing messages with recognizable logos and branding. Rather than creating an email from scratch, cybercriminals post the message as a screenshot, hoping that potential targets do not realize that they are looking at an image rather than a real email. Similar to the scam recognized by the FBI, the email will state that the target is about to be charged for a subscription, and that they should call a phone number that directs them to a phony representative, who ultimately attempts to convince the target to give them control over their device.

Phone-Based Phishing Scams, Also Known as “Smishing” and “Vishing”

- “Smishing” attacks share many of the same traits as traditional email phishing attacks. The text messages will attempt to make an emotional connection to the intended victims. Perhaps they will convey a sense of urgency to pay a bill or reactivate a service. Another attempt might tell a person that they won a contest and need to click on a link to claim their prize.

- “Vishing” is where a malicious actor tries to coerce their victim into revealing personal information, such as bank details and credit card numbers over the telephone. The sender will make the message appear as though it’s coming from a reliable source, such as a bank or other trusted institutions. This is an important distinction from other spam texts you may receive. A spam text message does not attempt to disguise itself as a trusted source. For it to be a “smishing” attack, the text message needs to appear as though it’s coming from someone you trust.

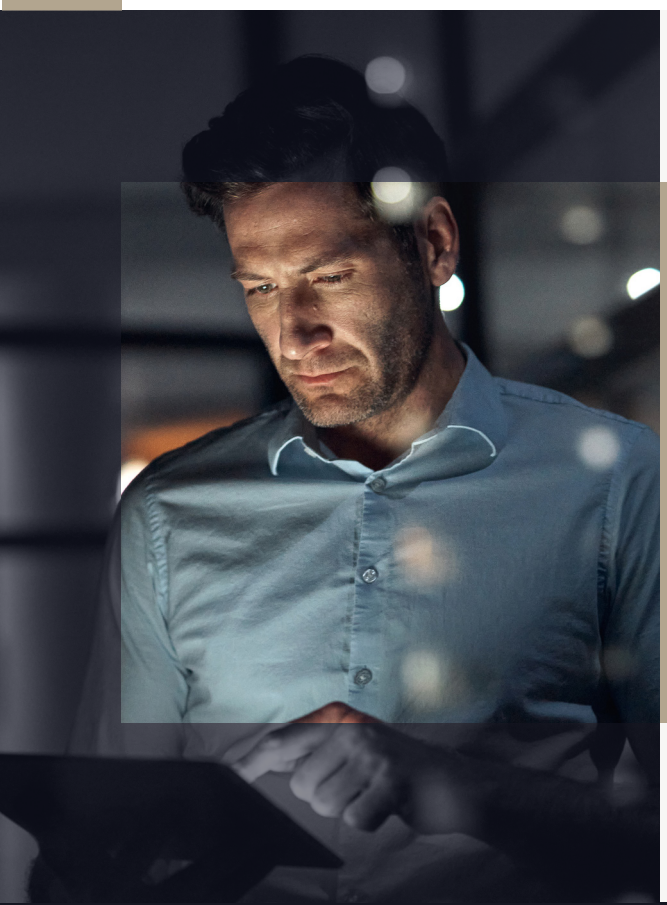
Cyber Scam Red Flags

1. The email in question wants you to take action immediately to remedy a problem, or appear to be threatening in nature. These messages will try and convey a sense of urgency to get you to act quickly without stopping to consider whether the problem or threat is legitimate.

2. The sender wants the target to turn over personal information, login credentials, or even money to fix this "problem." No legitimate entity will ever ask you for any of these data points under any circumstances.

3. If the malicious actor is posing as a legitimate entity, they may slightly change the spelling of the email domain to look as close as possible to the organization they are mimicking. They could do so, for example, by changing an O for a 0, or by using a .net email domain rather than .com.

4. The sender of the email asks for payments that are hard to track, such as a wire transfer, cryptocurrency or gift cards.



BlackCloak provides an application backed by 24/7/365 coverage that ensures our members protect their privacy, their devices, their homes and peace of mind. Our holistic and white-glove approach takes the complexity away while ensuring best-in-class security.

With BlackCloak as your trusted partner, you'll protect what matters most and have control over managing your cybersecurity and privacy risk – and your personal advisor will always be just a call, tap, or text away.

Reach out to your BlackCloak Account Executive:
Kerry Tary
kerry.tary@blackcloak.io

BLACKCLOAK®

Learn more at www.blackcloak.io