ATTORNEYS AT LAW

BULKLEY RICHARDSON

BETTER REPRESENTATION

VISHING SCAMS: A NEW CYBER THREAT IS ON THE RISE.

According to the Federal Bureau of Investigation ("FBI") and the Cybersecurity Infrastructure and Security Agency ("CISA"), cybercriminals have been waging a campaign to access company data through remote workers. This "vishing" campaign was launched in July and, according to the federal agencies, it is on the rise.

As described by the FBI and CISA, vishers first create a duplicate version of a company's VPN login page, often also registering a domain, such as "support-[company]" or "ticket-[company]." Then they review all publicly available information about an employee, which can be extensive, depending on social media settings, to prepare a socially-engineered attack.

Next, they contact the employee by phone, either using VoIP (voice over internet protocol) to remain anonymous or by "spoofing" a company number and making it appear that the call is coming from within the organization. In the conversation with the employee, they may pretend to be a member of the company's IT team, or another authorized individual, and indicate that they need the employee to log in to a "new" VPN connection. If this vishing campaign is successful, the employee will enter their credentials, including any required two-factor authentication information, into the visher's cloned page and send this information directly to the unauthorized party. In turn, this gives the visher more access to company data, which could enable additional vishing campaigns or a ransomware attack.

Federal authorities recommend several tactics for thwarting vishers. Monitoring domains with the corporate name could reveal copycat sites early. Restricting VPN access to particular hours could reduce the risk of unmonitored, after-hours "exploration" of your company data by hackers. Limiting employee access to sensitive information and monitoring activity on company servers could minimize the damage caused by successful vishing. Employees, for their part, can be instructed to verify the spelling of web links, to be alert to unsolicited phone calls, and to bookmark the correct VPN URL.

If you may have been the victim of a vishing campaign, you wish to update your WISP to account for this risk, or you have additional questions about how a remote work environment can impact your legal obligation to safeguard personal information, please contact a member of Bulkley Richardson's Cybersecurity Practice Group.

Lauren Ostberg

lostberg@bulkley.com
413-272-6282

Jim Duda

jduda@bulkley.com
413-272-6284

Scott Foster

sfoster@bulkley.com
413-272-6258

Michael Roundy

mroundy@bulkley.com
413-272-6254

David Parke

daparke@bulkley.com
413-272-6257

Sarah Willey

swilley@bulkley.com
413-272-6228