INSIGHTS

Cyber made simple.

one brightly cyber

SOCIAL ENGINEERING SCAMS TAKE A NEW TURN

BY JAY BORDEN

One of the most effective ways to penetrate any organization is social engineering. That is, fooling people into providing confidential information. Why is this so popular? Because it works! No technical skills needed. Just the ability to ask the right questions or provide enough information to fool someone into thinking you are authorized.

Research says people are the cause of anywhere from 65% to 90% of breaches. That is an alarming number.

Healthcare providers are prime targets for cybercriminals due to the extensive and varied information they keep. Health-related information plus name, physical address, age, email, credit card, insurance number, etc. This checks many of the boxes on the cybercriminals' wish lists.

The typical approach is for attackers to send someone an email or call them on the phone. Then request private information such as username and password, credit card number, or request they submit a wire transfer. Of course, you need to convince them you are authorized to request and receive that information, a company executive, a government official, IRS, a bank official, anyone who seems reasonable to request it.

Those methods work well. Now cybercriminals have a new way to exploit social engineering. Don't call an employee, call the IT Help Desk and convince them you are an employee, often in a financial role. The phone call is spoofed to show an originating number in a correct area code for the target company.

MFA, Multi-Factor Authentication, is typically used in these organizations. To get around this the caller claims their phone was lost or is broken so they can't receive the MFA authorization code. This means they can't log into their account to do their job.

onebrightlycyber.com
(888) 773-1920

SOCIAL ENGINEERING SCAMS TAKE A NEW TURN

CONTINUED

Of course, the Help Desk agent requests information to prove the caller is who they claim to be. But the attackers are prepared with information found on public sites including social networking sites or obtained on the Dark Web. They will have what is needed to prove identity, last four digits of the target's social security number, corporate ID number, etc.

It is enough to convince the Help Desk agent. The attacker requests a new device be added to the MFA function. Once that is done, the attacker can log in with no problems because it is a valid id. They then access the payer websites and submit the proper form for changing the ACH account to receive payments. ACH is the Automated Clearing House, the entity that processes the payments.

Next is to send emails to the payment processors, like insurance companies, changing the account number to receive payments to the one they just created. As soon as funds are received into the new accounts they are sent overseas where the funds can't be retrieved or recovered.

In one case, to add credibility to the scam, attackers registered a new domain with a one-letter change from the target organization. An email account was created on the new domain with the same username as the target entity's CFO, Chief Financial Officer. Emails sent from this account appear to come from the CFO of the target company.

What to Do?

Be sure Help Desk agents are required to call the supposed employee using the phone number on file. Of course, the scam caller may request a new phone number be used saying they are out of the office, or their phone was lost. Those tactics must be ignored no matter how persuasive the caller may be.

But the first thing to do is train the Help Desk staff about these types of attacks. Use fake phishing emails and calls to see who takes the bait.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.