PHONE PRE-TEXTING: MASTERING SOCIAL ENGINEERING SAVIOR-FAIRE

Adding a Little More Science to the Art of Phone Pretexting
What This Presentation Is

This is not a focus on the infrastructure setup, though there is a little of that. Our main focus is the general flow of setup and the preparation and skills needed to hone the social savoir-faire for success at the phone pretext.
The Kick-Off Call

It begins with the client kick off call

• There is a vast number of ways to play this, determine what the client deems as criteria for success, they may be looking for very different things based on the industry, save time by figuring out their comfort level on the kick-off call

• Are they comfortable with impersonating a current employee? Some are not since it could lead to confusion down the road

• Are they comfortable with you going for a screen connect (or similar) session?
OSINT

We want to know:
• How large is the company?
• How large is their IT staff?
• Who will you impersonate?
  • Choose based on title; the lower the better
• Current status with company; use other social media and jobs sites to confirm employment status
Example Scenario

For this presentation, the example scenario will be the Helpdesk impersonation to get the user to “sync back up with the server.”

• The script
  • Super easy to read, with components that change highlighted and focused on
• The domain
  • The most important part of this whole operation; must be:
    • Easy to say over the phone
    • Use a recognizable subdomain
    • Non-suspicion arousing in the least, which might not mean what you think
• The portal
  • Simple, clean
  • A full clone is nice but not always possible
  • Not nearly as important as the domain you choose
  • If it can be avoided, do not volunteer the exact address of the portal to the POC, they LOVE blacklisting it on their side
Example Script (with less spacing than the real script):

• Hi <name>
• This is First and Last Name from the Service Desk, how are you doing?
• <response>
• Last night we tried pushing some updates out to the workstations and it looks like yours went out of sync with the update server and didn’t receive them. Do you remember denying any updates yesterday or today?
• Do you have a moment to assist with getting it corrected? It should only take a minute or two.
• <response>
• In a browser, you can use any browser on your machine, please go to https://businessname.yourdomain.com
• This is a web portal that IT has setup to assist in re-enrolling in automatic updates.
• As you know, the Service Desk will never ask you for your password, so you will need to login yourself to re-sync with the update server.
• You may receive a push notification in a minute or two, please accept that when it comes through.
• <wait a few seconds>
• Okay, it looks like we’re all set here. Thank you so much for your time, have a great rest of your day!
Successfully enrolled in the [redacted]. Please check your email for the next steps. You may now close out this page.
Making the Calls

• Get into character
  • You are just a regular person doing their job at the same company as your target; be casual, be natural, speak as they would
Quality of Life Tips

- Get a group together to make the calls a competition
  - Changes nervous energy into fun energy and makes you sound better and more natural
- Keep a log organized from the start; don’t record things separately
Success! Now What?

If post-exploitation is in scope, you could:

• If they have MFA, use the credentials you gathered while on the phone with the target to login and trigger the MFA token on their side, preparing them for that on the phone
Questions?