81 Mill St., Suite 300 Gahanna, OH 43230

Attention:

New Cyber Security Threat
Government Official Fraud

From the Desk of Bill Wright:

FBI warns of increased cases of people posing as Government officials to discuss a cyber security issue . . .
Don't think it can happen to you, here in central Ohio? Read about a local business owner's story . . .

Have you heard about the latest way cybercriminals are targeting small to medium sized businesses across the country, just like yours?

The FBI announced they have seen a significant increase in the impersonation of government officials contacting businesses to discuss a 'security concern', usually related to that company's technology.

The timing of this announcement is interesting, as I had a 'project only' client (we did a single project for them over 2 years ago and they "*Didn't need continued monitoring*") reach out to us earlier this week because an agent from the Department of Homeland Security (DHS) called to setup an appointment to discuss a security concern for their on-premises Exchange (email) server. She sounded very professional and official – she even sent an email outlining the security concerns, that also included her contact information.

Before I go too much further, I do want to say we are still investigating all of this… BUT everything she said and sent looked legit. The email was clean (no malware), and the PDF attachments were clean, as well. Things looked like the real-deal - except for the email signature that had the local DHS address and Fax number, but only listed a direct contact number. Again, the email appeared to be legit, sent from a legit DHS email server and everything.

The business owner asked us to run some tests and we found a few things, but nothing that the DHS agent had claimed needed to be investigated to pursue 'the bad guys' that had gotten into this company's Exchange server. I told him to call the local DHS office to verify the agent, and then to not keep the appointment until everything about her and the issue was in the clear. He called the number in her email … no answer, no voicemail, no DHS announcement, it just rang and rang. He got busy and didn't call the local DHS office. She didn't show up for the appointment and she hasn't reached out since.

So, last night I get a panic call from this business owner, "All my files say they are locked, what do I do?"

Maybe you see where this is going.

That's right.

His entire server has been locked up with Ransomware. I ask him, "When was your last backup?"

"I don't have a backup."

These few words are every MSSP's worst nightmare, and they should be yours as a business owner, no matter your industry, too.

I had to do what all of us MSSP's hate doing – I had to tell him there's very little I can do at this point to help him recover his data. To be very frank about the conversation I had with him, I had to share the terrible reality that he will most likely have to pay the ransom asked of him by the cybercriminals responsible OR recreate everything. And I mean *everything.* Even if he pays the ransom and does get his files unlocked, everything will still need to be redone. The server will have to be wiped and hard drives replaced (at an absolute minimum), software will need to be reinstalled, among other technical things, and, probably most impactful to him as a business owner, he will be down for a *significant* amount of time.

While we are still putting things together, the timing of the DHS agent's call, then not being able to contact her and not hearing anything more from her, followed by the encryption of his company Exchange server only a few days later…

Sure, it could just be coincidence, but I must say, it is all *very* suspicious.

I want you to know, I'm not sharing this to scare you**.**

I am, however, sharing to make you aware this DOES happen, right here in central Ohio, and also how crafty an attacker can be to make everything sound and look legit.

So, if you hear from a 'government official' to discuss a security issue with your company's technology… be very careful and verify everything they tell you with the agency they're claiming to represent.

As always, if you have any questions about or concerns with your cyber security status, give me a call. I'd be happy to review what we have in place for you at your earliest convenience. If you're not yet a client of ours, still give me a call and we can discuss what you have in place currently, what isn't working about it, and what could better address your needs.

Have a tremendously great day and do be safe out there!

MCPS | MCNPS | MSSP
Founder, CEO & Chief Creative Officer
WCI Technology Solutions