SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

A normal week on the cyber battlefield.

Friday was the first of December, 2017, the end of a typical work week. No holidays, no major crises, just a run-of-the-mill typical week.

So here are just some of the cyber-related activities I encountered since the previous Sunday:

1. Phishing attack – On Tuesday morning, November 28th, at 11:25 GMT+5, I received a call from an 800 number on my cellphone. Upon answering the call, a computer-generated male voice (or pre-recorded voice) authoritatively advised me that, "*This is Verizon Account Services, your account has been suspended for account verification. Please enter your account billing password on your keypad now to continue*." I immediately hung up the phone, and dialed back the number displayed on the Caller ID. The number turned out to be AT&T Customer Service.

   Now, I'm not a big fan of AT&T but I do know, without question or doubt, that AT&T is **NOT** going to steal Verizon customer passwords. This was clearly a phish. So, I called Verizon to report it as fraudulent activity and to get them to trace-back the incoming call.

   The customer service representative was perplexed. She wasn't sure how to escalate the issue and after being on hold several times and speaking to two different representatives

over a 70-minute period, Verizon finally asked me to text their SPAM Advisory account (7726) all the information I had shared with the representatives.

After I finished, I marveled at how ill-prepared Verizon was in dealing with a reported phishing incident. Verizon, a top cyber-security firm in its own right, with a brilliant CISO, hadn't a clue as to how to deal with the situation. The second thought that came to me was that perhaps as many as 90% of people who would have received that phone call would have actually entered the billing password – thus compromising their accounts.

As of Friday, December 1st, I have not heard a word back from Verizon.

2. Bank/Wire Fraud issue – Two weeks ago, my manager of communications from the non-profit institution of which I am president, contacted me regarding an urgent call from someone in Albuquerque NM. This individual had applied for a job on monster.com and received a package from the job-posting site with my institution's name and address as the sender. Additionally, he claimed there was a check that he was to deposit and instructions on sending money to one of six individuals in six different cities – all purportedly tied to my institution. He demanded a call-back from an official of our organization to explain.

   Instead, I contacted my attorney for best advice on how to proceed (my feeling was to reach out directly to the FBI). Instead, my attorney recommended we contact the local police department, as he felt they would have a specific protocol for this sort of issue. We did, a report was filed and we went into wait mode.

   Then, on Monday November 27th, our office received a package that had been rejected by its intended recipient and was marked "Return to Sender" – the sender being listed as my organization. Our office manager opened the package once she ascertained that no one had sent it and found a letter and check with similar instructions to what had been reported the previous time.

   When she contacted me, I told her to immediately call the police and file a 2nd report. She did so and we are back in wait mode. In the meantime, there is a cyber-criminal out there, using my organization's good name for nefarious purposes.

   Once again, I'm struck by two issues. First, the police department may have protocols around this type of crime, but there is little to no communication back to us, a victim, about what is happening. Second, I'm left wondering how many people out there have fallen victim to this scam, getting financially harmed, have had their PCI and PII breached – and think my organization is responsible.

   Just a typical week.

Knowledge and awareness are your best defense!
Please follow me on twitter: @stevewertheim