Social Engineering Attack Targeting Conference Attendees

"Amateurs hack systems, professionals hack people." - Bruce Schneier. American cryptographer

It started on a regular work day

An employee receives a phone call at work from a familiar organization asking to confirm information about their credit card account and in their trusting nature, they provide the information. The problem: They just fell victim to a social engineering attack. Now the organization's data and finances are at risk.

People often represent the weakest link in the security chain

Social engineering is a psychological manipulation technique that persuades victims into revealing sensitive information to gain access to systems, data, or finances. Instead of an attacker searching for software vulnerability to exploit, they take advantage of human psychology. A hacker might fabricate trust with an individual and ultimately convince them to share access credentials to systems or wire funds, for example. Social engineering attacks tend to target individuals who have special access to these assets.

Happening to conference exhibitors

Recently, we at Bonefish Systems received a phone call at our office from a private number stating they knew we are signed up for the OSBA conference in November. The fraudster, who provided his name as Roman Michael Woods had said their company name is Convention Experts based out of Boston, MA and urgently tried to convince us that they had a deal with a hotel for the upcoming convention. However, to receive the deal, we would have to provide our credit card information.

Once we became certain that this was not a legitimate call, we made the fraudster aware that we were reporting this to OSBA to ensure others are aware as well of these calls occurring. The fraudster became very defensive and angry which was another sign that we were correct in our suspicions along with the fact that there was not a valid website for Convention Experts.

Social engineering prevention

Social engineers and fraudsters manipulate human emotions to carry out their schemes and prey on trusting employees and individuals. Therefore, be cautious whenever you feel alarmed by an email or phone call and when you are attracted to an offer displayed on a website/link. Consistent training tailored for your organization which includes demonstrations of ways attackers might attempt to trick your employees, is a crucial defense against these attacks.

The following tips can help improve your vigilance in relation to social engineering hacks.

- Don’t open emails and attachments from suspicious sources
- Password management - update passwords often
- Ask potential imposter questions to verify identity - Ex: "What's your business's address, website, etc?"
- Ask yourself questions. Ex: "Am I being pressured to act fast?"

If you’d like more information or training on social engineering attacks, please reach out to Bonefish Systems.

Info@bonefishsystem.com
614- 427- 3827