Social Engineering: How to Avoid Becoming a Victim

By Robert Gentry, senior consultant, information security services
Sollievo Group, LLC

Time and time again, the credit union movement prides itself on the notion of "people helping people." It's our employees providing the most outstanding quality service in service of our members that sets us apart from banks. Credit unions are all about people.

It's in our nature to try and be helpful to members and take people at their word. Unfortunately, the weakest link in every security program is the human and hackers use these inherently accommodating characteristics to their advantage. They look for vulnerabilities in our front lines - our employees - to steal sensitive information through social engineering.

Social engineering is the act of manipulating people to divulge confidential information. The bad guys exploit human psychology to get the information they need for their criminal enterprise. Although this has been occurring since long before the development of information technology, the social engineer can now operate on a global scale with anyone who has a data connection. And like a lion on the hunt, the social engineers target the potential victim.

The exploitation of certain human behaviors have proven time and time again to be successful in persuading people to surrender confidential information or otherwise fall prey to criminal manipulation. Social engineering can happen through email or over the phone, and could also take place in face-to-face interactions. Maybe a maintenance worker you don't recognize has gained access to your building or an email was sent from someone posing as a member asking for the account number that they "forgot."

Now here's the big question. How can your credit union keep employees from becoming victims of social engineering? Here are some things to keep in mind:

- **Slow down.** We all are rushed and pressed for time. The bad guys are counting on you to click first and think later.

- **No one is immune, although we may think we are.** Smart people do not fall for this, right? The bad guys use many or the same tactics as legitimate marketing to influence your behavior. You do not want to buy their product.
- **Convenience often trumps security.** Most of us have sat through many security awareness sessions. We know what to do but it's a real pain and, really, who's got time for that? A prime example is the use of unique passwords for sites we access. But they can be so inconvenient and hard to remember. Recently, there was an article about a victim whose bank account was emptied while using the Starbucks app because that person used the same password for most of their accounts. In addition, password lists are available for sale on the dark net so social engineers can get them without your knowledge.
- **Be wary.** Sweet talkers can be flattering, certainly. The bad guys know that and are ready to turn on the charm. Just be on the defensive when those sweet nothings come rolling in - they want something, but you don't have to give in.
- **Stay calm and don't panic.** If you get solicited to provide passwords and other security information, stay calm. The bad guys are hoping you will give up the gold, but take a minute to slow down and think. Do I know the person who is asking for this information? Why do they need it?
- **Control your curiosity.** The unsolicited email arrives and we are just curious to see what it's all about. The bad guys know we are curious people. Resist the temptation, delete and move on.
- **May I help you?** Credit unions are in the business of helping their members and we naturally want to be helpful. The bad guys need our help too. Maybe we should think twice before unlocking the online account for that polite member. Are they who they say they are?
- **Get rid of the "nothing is going to happen" mentality**. The bad guys love organizations and people that become complacent concerning security awareness. It's easy to fall into the trap of nothing has happened in the past therefore nothing will happen in the future. This false sense of security is very dangerous. The threat is real and constantly evolving. Security awareness is a continuous and dynamic process. A little healthy paranoia can be a good thing.

Social engineering is everywhere, and it's not going to slow down. Credit union employees should always be on their game. Make your staff aware of these tips, and stay one step ahead of the social engineers.

About Robert Gentry

Robert Gentry is a senior consultant of information security services at Sollievo, the risk management CUSO of Vizo Financial Corporate Credit Union. He may be reached at (855) 605-5664 or seniorconsultant@sollievo.com. Robert Gentry brings more than 20 years of experience in the information technology field to his role as senior consultant. Throughout his career, he has been responsible for server and network administration, firewall and security administration and IT management. As part of the Sollievo team, he performs information security risk assessments, security awareness training and incident response planning for credit unions.

About Sollievo

Sollievo Group, LLC is a wholly owned CUSO of Vizo Financial Corporate Credit Union located. Sollievo (pronunciation: solˈljɛvo), an Italian word that means relief, offers a comprehensive collection of risk-management products and services to credit unions. Sollievo's mission is to provide peace of mind and help meet compliance obligations and improve the overall risk posture of credit unions. Services include enterprise risk management, information security services, training, business continuity services, and more. For more information, please visit www.sollievo.com.