FIRSTCALL

Corporate Security & Advisory Services

SOCIAL ENGINEERING : POTENTIAL THREATS TO BUSINESS EXECUTIVES

TABLE OF CONTENTS

FIRSTCALL

Corporate Security & Advisory Services

Introduction

In today's society, it's not all that uncommon to read stories in the news about business executives who have found themselves scammed, phished, robbed, or, even worse, kidnapped for ransom. While not in every case, an executive security plan that doesn't contain protection against social engineering is often to blame.

Wanting to stay transparent, many executives willingly share information[1] about their private lives through social media sites. However, this leaves them vulnerable to attacks. Not only do personal posts put people at risk of having their information hacked, but this type of information sharing can also put them at risk of physical danger.

Social media sites like Facebook, LinkedIn, and Twitter provide a forum for open discussion and information sharing. They also provide cybercriminals an opportunity to gather data they can use against the person posting. There is nothing wrong with executives talking about their private lives on social media platforms. But in doing so, they need to understand that this practice helps facilitate attacks against them whether online or in person.

Safety goes beyond just knowing that risks exist. Business executives need to learn the telltale signs of social engineering and take the appropriate measures to protect themselves and their families. The good news? Making small adjustments to social media accounts and the way that executives post information is usually enough to dramatically improve security.

1 https://www.cso.com.au/article/625104/social-engineering-how-your-employees-helping-attackers-steal-your-data

What is social engineering?

While some people have never heard the term "social engineering,"[2] it entails actions that have been around for a long time. In layman's terms, it is a form of attack that uses human interaction and, often, manipulation. People who use social engineering techniques take great care to hide their true identities. In fact, they initially conceal their motives, which is what makes them so dangerous.

With social engineering, a cybercriminal uses different methods to get a business executive to pull away from standard security practices and procedures. By coming off as friendly or genuinely interested in an executive's company, products, or services, they slowly break down barriers, allowing them to access information, networks, finances, and even brick and mortar locations.

Simply put, social engineering exploits innocent people. While different cybercriminals use this tactic to garner information, hackers[3] are particularly fond of it. Regardless, the goal is to find the target executive's weaknesses, which puts that individual's company, network, software programs, products, services, and/or family at risk.

Implications for cybersecurity and physical security

Social engineering has a direct impact on both cybersecurity and physical security. Consider the following example. A business executive who believes in total transparency shares information about a new product getting ready to launch. Suddenly, someone who shows significant interest starts or joins in on the conversation around that product. That person has likely conducted in-depth research in order to sound as though they understand the industry and share in the excitement of the product rollout.

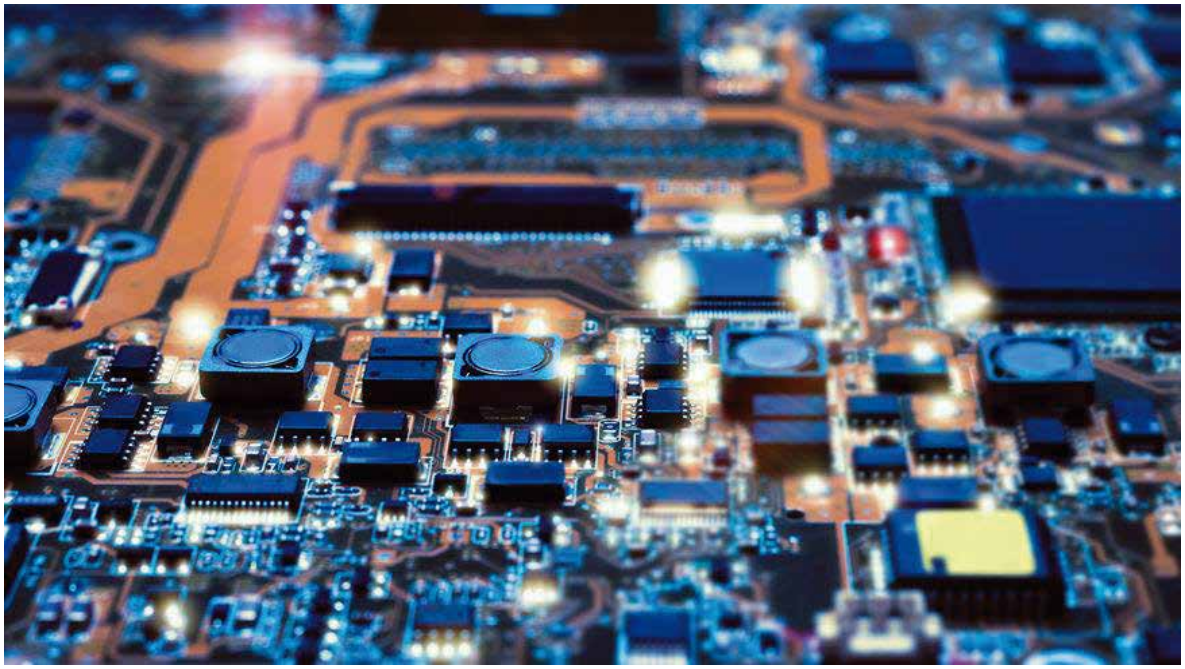
2 https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering
3 https://searchsecurity.techtarget.com/definition/social-engineering

Unfortunately, that individual is nothing more than an actor. They are playing a role to convince the executive to divulge privileged information. They might try to wiggle their way into the organization by pretending to offer incredible value. Eager to discuss the new product, the executive becomes more willing than usual to tell all. Quickly, what seemed like an innocent exchange with a trustworthy person turns into something destructive or dangerous.

Now knowing the inside details of the new product, the cybercriminal could blackmail the executive to force the sharing of proprietary information. For someone extremely devious, the individual using social engineering tactics could go as far as threatening to do bodily harm to the executive's family to get what they want.

The vast amount of information online makes social engineering challenging to fight. However, it is not impossible. Along with social media sites, people who use this method can find tons of details on any given business executive by watching YouTube videos, reading news articles, listening to interviews, and so on. Without giving any thought to a threat, executives often reveal much more than they should.

Consider a targeted business executive planning to travel with their family for a nice weekend getaway. In anticipation of the upcoming trip, the executive shares details about hotel accommodations, planned excursions, and the date of departure and arrival back home. Within minutes, a cybercriminal has everything needed to carry out a plan to harm the executive and perhaps the family.



Executives often share itineraries online, which seems innocent enough. However, that gives a cybercriminal the data needed to plan an attack. The cybercriminal could also be a recently terminated employee eager to get revenge. Without doing any digging, that person knows when and where to go for retaliation.

With social engineering, the possibilities are endless. This is why every business executive needs to learn the signs of trouble and take the right steps for optimum protection.

Reducing social engineering threat

Fortunately, business executives have options[4] for reducing the threat associated with social engineering.

- Less Sharing – While probably difficult, especially for executives who live and work by the rule of remaining transparent, it is imperative to share less information, regardless of the medium. They can still share information, just nothing that could come back to haunt them at some point.

- Personal Information – It is possible to share pertinent information to build a successful business without giving up personal data. Business executives should scour their public domain accounts, scrubbing them of any private details.

- Advanced Technology – All companies, regardless of size or industry, should have a secure email system[5], including web gateways designed to scan for social engineering tactics and anything malicious. Business executives should also consider taking security awareness training and offering this to the entire organization. After all, cybercriminals often look for weak points from which to gather information, such as through lower-level employees.

Take Control

Just because social engineering is a real threat does not mean you have to become a victim of it. Take charge today by understanding the different tactics that cybercriminals use. Then, find the best way to protect yourself, your family, and your business.

4 https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

5 https://www.computerweekly.com/feature/How-to-reduce-the-risk-of-social-engineering-attacks

ABOUT FirstCall CSS

FirstCall Corporate Security and Advisory Services is a global business advisory and risk management company providing personal protection, workplace stability, and crisis advisory services to Fortune 1000 corporate security departments and family offices. With 25 years of experience in emerging and high-risk markets plus regional offices in 16 strategic locations around the world, FirstCall delivers confidence and peace of mind by providing experienced and trusted security professionals. FirstCall provides highly personalized solutions in response to the challenges of doing business in today's fluid, global marketplace.

- 25+ years of experience solving complex security problems on a global scale.
- Global capability built through an international presence.
- More than half the Fortune 100 served.
- In-depth understanding of social, political, and economic conditions in each market we serve.
- Proven ability to attract, train, and promote the most talented professionals in our industry.

Interested in learning how FirstCall can help you mitigate your security risks? Contact us today at:

FirstCall Corporate Security and Advisory Services
One Sansome Street
Suite 3500
San Francisco, CA 94104 - USA
Phone: +1 (415) 781-4300
Email: mktglobal@firstcallcss.com

FIRSTCALL

Corporate Security & Advisory Services

FirstCall CSS
Worldwide Headquarters
One Sansome Street
Suite 3500
San Francisco, CA 94104 USA

+1 (415) 781-4300
mktglobal@firstcallcss.com
www.firstcallcss.com

CSS-2021603