# Quid Pro Quohttps://blog.drhack.net/social-engineering/2/

In Latin, quid pro quo means “something for something”. In social engineering, an attacker who uses quid pro quo promises a benefit (can be a form of a service) in exchange for information.

One of the most common quid pro quo methods involve attackers who impersonate as IT service people. The attackers will call as much number as they can find to offer IT support with the hope that there is a victim who has the same problem and needs help [David Bisson]. When the attacker finds his victim, he will pretend helping solve the problem and either ask the victim for personal information or trick them to install malware which requires the victim bypass his anti-virus softwares.

Another way of using quid pro quo which doesn’t require complicated methods such as calling every number to find a victim, the attackers can just simply create a survey and convince victims to share their information in other to win a prize (sometime the prize is really simple such as a pen or a bar of chocolate) [David Bisson]. This attacking method seems simple and easy to avoid. However, in the modern society where most of us cannot live with out the Internet and social networks, people get used to exchanging their personal information for awards and recognitions, which makes this attack effective.

# Pretexting

Pretexting is another form of social engineering - probably the form that most people have encountered - where attackers create a fabricated scenario in order to obtain victim’s personal information [M Salman Nadeem].

Most of the time, attackers impersonate authorities such as police, insurance investigators to make the scenario more serious. One example which came from my landlord’s friend is his friend’s wife received a call which announced that her husband won a lottery, therefore they needed her husband’s phone number. A couple days later, she received a call from her husband’s number. However, the other side wasn’t her husband but declared himself RCMP officer. The caller announced that her husband had been arrested so in order to bail him out, the wife had to transfer an amount of money into an account number. Fortunately, her husband was sleeping upstairs. Therefore she knew that was fraud and didn’t fall for that. There was a time when my former employer received a call announced that there was something wrong with his account so he had to bring his bank card to a specific location in order to get it done. However, he knew the call was just a fraud because the address that the caller required him to go to was a household address.

Another form of pretexting attack is emailing. Attackers will send emails - which are fabricated to make an expression that the emails come from authorized organization such as banks or government organizations - to victims and these emails will require victims enter their login information. This form of pretexting attack and the form of tricking victims on phone are similar to scamming and quid pro quo. However, pretexting doesn’t promise any award or try to get victims click on to something, instead, pretexting attackers build their trust with their victims by impersonating authorities (most of the time, the attackers create fear and urgency which have a huge effect on human in terms of psychology). Once the trust is built, attackers can easily obtain their victims’ private data.

# Tailgating

Tailgating or “Piggybacking” is another type of social engineering which is used specifically to get entry to a restricted area secured by electronic access control [M Salman Nadeem]. The goal of this method is to steal valuable property or information inside that area.

The main factor which makes this method successful is it exploits courtesy. A common scenario is when the attacker disguises himself as a delivery guy and waits in front of the restricted area. When an authorized person gets access into the area, the attacker will follow and ask the person to hold the door for the attacker. By courtesy, the authorized person will hold the door by which the attacker gains access into the area. In more sophisticated scenarios, the attacker may try to trick the victim by creating an uncomfortable situation or providing a fake piece of identification.

However, this type of attack is less effective than other types. Most of the time, people learn about tailgating from TV shows and movies rather than run into a realistic case. In large size organizations, authentication stage is really serious which makes this attack impossible to perform. In small size companies where staffs know each other well and know how their business operates, it’s hard for an attacker to gain access into the area without causing any notice. This method may work in places where the number of staffs changes regularly because it takes time for these employees to know each other and know how their workplace operates. An example which comes directly from my workplace. The process of firing and hiring occurs so frequently that managers don’t change the passkey to employees’ room, which creates access for not only current employees but former employees who can just come to the workplace as customers.

# Baiting

Baiting is a type social engineering which focuses on human curiosity by using physical items such as flash drives or CD-ROMs. When the victim uses these devices on his computer, he will install malware or ransomware inadvertently, which grants the attacker the ability to control the system or exploit it.

To make the attack more effective, the attacker can disguise his baits with company logos or titles which create curiosity. Similar to tailgating, this type of attack seems unrealistic and can be seen most of the time on TV shows and movies. However, in 2008, there was a serious cyberattack against the U.S military which came from an infected flash drive put in a laptop [the CNN Wire Staff]. In 2016, a social experiment was proceeded in which 200 USB sticks were dropped in public places and surprisingly, almost 20% of them were picked up and plugged into a device [Ben Kepes].

This method is dangerous because it takes advantage of curiosity and greed which some people cannot resist. In addition, this attack doesn’t require victims to provide information or click to a link. When the infected device is plugged into a computer, an auto-run script will run automatically and grant access to the attacker.

# How to Protect Yourselves from Social Engineering Attacks.

# Quid Pro Quo

There are a couple methods to protect yourselves and they are easy to implement. One general rule which can be applied on all methods is never give personal information to unauthorized person or organizations, especially over a website because even government organizations are not allowed to asked for private information via emails or phone calls. There is an exception that when you buy something from websites like kijiji or usedregina, you may have to give your address or phone number in order to process the transaction with buyers or sellers [M Salman Nadeem]. In that case, you are aware the risk of giving away your information.

If you receive a call and the caller says he(she) is from a trusted organization, call the company back using a publicly posted phone number from their website [M Salman Nadeem]. Or if you are suspicious about the call, just cut it off.

In conclusion, if something is too good to be true, it is a 100% scam.

# Pretexting

Pretexting methods are difficult to recognized and therefore harder to defend against.

One way that can make your personal accounts more secure is avoid using well known information such as your mother’s maiden name for passwords or backup questions since these information can be obtained easily. Instead, use information that is familiar to you but almost no one knows such as the name of your first pet or first name of your teacher in fourth grade [“Avoid Pretexting And Protect Your Personal Privacy”].

Similar to Quid Pro Quo, unless you initializes the contact, never provide private information over the phone or internet. Besides, with the development of social networks, attackers can find your information from your friends or relatives’ social network accounts. Therefore, your friends and relatives need to know the importance of privacy and protecting personal information in order to protect you and them.

# Tailgating

Preventing an unauthorized person who appears as a technician or delivery guy to enter a building is sometime difficult, especially at the time when many people arrive at the same time. However, there are some methods which can be used to prevent tailgating.

Authorizing each person when they enter the building by using receptionist, RFID scanner or biometrics such as fingerprint reader or iris scanner [Rajeev Kav]. In addition, surveillance systems can be installed at the entrance or inside important areas to manage the access to and from those areas.

Restricting accesses to the organization’s important information by setting up password for printers, computers and internal wifi network so that if attackers successfully enter the organization, they cannot access to its private information.

# Baiting

The key to prevent baiting is to recognize it. However, sometimes baiting gets complicated to identify as it can come from a seemingly legitimate form such as a free gift or software update. Therefore, the best method to defence against baiting as well as any other social engineering attacks is education and training. Organizations need to train their employees by case studies, exercises or what-if scenarios in order to recognize and prevent baiting. Companies can also propose a policy that restricts foreign devices plugged into company’s system or these devices have to be approved from administration team [“Social Engineering - Would You Take the Bait?”].

The main target of baiting attackers is people who have less or no knowledge about information security. Therefore, everyone should do open discussions with her family and friends in order to make them aware about the dangerous consequences of baiting attacks [M Salman Nadeem].

# Social Engineering vs Laws

Large size corporations and organizations often purchase insurance coverage in case a cybersecurity incident happens. However, the loss cause by social engineering fraud does not meet the requirements of these coverages, which creates a significant gap in coverage under a crime policy for these types of cyber risks [Camille Dunbar].

This situation was the result of one of the first social engineering fraud cases in Canada - The Brick Warehouse LP v. Chubb Insurance Company of Canada - where the Alberta Court of Queen’s Bench decided that the loss of Brick Warehouse LP did not fall within the terms of crime policy coverage. A Brick employee received a phone call from a person claiming to be one of Brick’s supplier - Toshiba. By convincing Brick’s employee that he was a new employee, the attacker obtained information about the payment process. Later on, the attacker requested that all the payment for Toshiba had to be made to a new bank account. As requested, a Brick employee changed Toshiba’s bank information on the payment system using standard procedure. No one from Brick verify the change or contact either Toshiba or the bank to confirm the change. As the result, the amount was transfer to the attacker’s account was over $338,000. The fraud was discover later, but the Brick was able to recover only $113,847. Since the Brick was under a commercial crime policy by Chubb Insurance Company of Canada, the Brick made a claim for the money that couldn’t be recovered [Camille Dunbar]. However, Chubb denied the claim because the situation was not under the fund transfer fraud coverage and the court agreed with Chubb.

The court’s verdict was based on a similar case in the U.S - Taylor & Lieberman v. Federal Insurance Company, 2017 WL 929211 [Martin Kratz]. The situation was similar to the case in Canada when an employee wired company’s money to the attacker’s account after receiving a fraudulent email. In both cases, the request for insurance coverage was denied because according to court’s verdict, although those employees were not aware that the email (or phone call) was fraudulent, they did know about the transaction, which made the companies not eligible for coverage.

These cases show that social engineering fraud is a complex issue and most of the time not covered under commercial crime policy in insurance companies. Therefore, to avoid severe consequences caused by social engineering fraud, employers need to train their employees as well as review carefully terms and conditions when choosing an insurance company.

# Work Cited

Bisson, David. “5 Social Engineering Attacks to Watch Out For”. *Tripwire.* 23 Mar 2015. Web. 8 Apr 2018. URL: <https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/>

Nadeem, M Salman. “Social Engineering: What is pretexting?”. *Secure and private email service.* 30 Jan 2018. Web. 8 Apr 2018. URL: <https://blog.mailfence.com/pretexting/>

Nadeem, M Salman. “Social Engineering: What is Tailgating?”. *Secure and private email service.* 30 Jan 2018. Web. 8 Apr 2018. URL: <https://blog.mailfence.com/what-is-tailgating/>

Nadeem, M Salman. “Social Engineering: Quid Pro Quo attacks?”. *Secure and private email service.* 2 Jan 2018. Web. 8 Apr 2018. URL: <https://blog.mailfence.com/quid-pro-quo-attacks/>

Nadeem, M Salman. “Social Engineering: What is baiting?”. *Secure and private email service.* 7 Mar 2018. Web. 8 Apr 2018. URL: <https://blog.mailfence.com/what-is-baiting-in-social-engineering/>

The CNN Wire Staff. “Cyberattack in 2018 prompted new Pentagon cyberdefense plan”. *CNN.* 25 Aug 2010. Web. 8 Apr 2018. URL: <http://www.cnn.com/2010/TECH/innovation/08/25/pentagon.cyberattack/>

Kepes, Ben. “Here’s what happens when you drop 200 USB sticks in public”. *ComputerWorld.* 5 Jan 2016. Web. 8 Apr 2018. <https://www.computerworld.com/article/3002703/security/some-scary-insights-into-cybersecurity-risks-or-what-happens-when-you-drop-200-usb-sticks-in-public.html>

“Avoid Pretexting And Protect Your Personal Privacy”. *How To Vanish.* 27 Aug 2009. Web. 8 Apr 2018. URL: <http://www.howtovanish.com/avoid-pretexting/>

# 

Kav, Rajeev. “A Foolproof Strategy to Prevent Tailgating in your Building”. *Claudastructure.* 9 Jun 2017. Web. 8 Apr 2018. URL: <http://cloudastructure.com/blog/a-foolproof-strategy-to-prevent-tailgating-in-your-building/>

“Social Engineering - Would You Take the Bait?”. *Dara Security.* 03 Feb 2015. Web. 8 Apr 2018. URL: <https://www.darasecurity.com/article.php?id=32>

Dunbar, Camille. “Canada: Social Engineering Fraud: Significant Coverage Gap Under Commercial Crime Policy”. *The All Group LLP.* 6 Sep 2017. Web. 8 Apr 2018. URL: <http://www.mondaq.com/canada/x/626468/Insurance/Social+Engineering+Fraud+Significant+Coverage+Gap+Under+Commercial+Crime+Policy>

Kratz, Martin. “Cyber Security - When Social Engineering Fraud Is Not Covered Under Your Insurance Policy”. *Slaw.* 23 Aug 2017. Web. 8 Apr 2018. URL: <http://www.slaw.ca/2017/08/23/cyber-security-when-social-engineering-fraud-is-not-covered-under-your-insurance-policy/>