Call Center Scams

How call center scams work and how to avoid falling victim

Have you ever received a call about your cars extended warranty? Or perhaps from a company posing to be an IT solution about your computer that needs fixing? In today's everchanging, technological landscape, the reports of scam calls have been growing at an unprecedented rate, leading to millions of individuals falling victim each year. Falling victim not only leads to potential financial losses but also can lead to emotional and mental distress for targets. By understanding how these scams work, individuals can be better prepared to recognize their tactics and take the proper steps to defend against them.

What are Call Center Scams

Call center scams are large fraudulent operations where bad actors pose as a 'trusted entity' like insurance agencies, tech support, law offices, or tax agencies, to trick victims into providing sensitive information or access to financial accounts for financial gain. Often posing as reputable organizations, the scammers attempt to create a false rapport amongst victims by using social engineering tactics to gain the individual's trust. Once an individual begins to trust the caller, the scammer will then manipulate them for financial gain which can take form in a variety of different tactics.

Common Tactics Used by Scam Call Centers

- **Impersonation Scams:** These scams are the most prevalent tactics within the industry. Scammers will pose as a 'trusted entity' like a bank or government agency, to gain the target's trust and then trick them into providing personal information over the phone. Some of the information they might request is bank account numbers, SSNs, password information, and more. Never provide personal or financial information to an unknown caller. Unsolicited calls from legitimate organizations will not ask for sensitive information over the phone. It is best to hang up and contact the legitimate company directly using their verified contact method.
- **Tech Support Scams:** Often, scammers will pose as technical support representatives from well-known companies (Microsoft for example) claiming that the target's computer is infected with a virus or malware and requires remote access to fix the issue. Many times, they will use complicated technical jargon to sound legitimate to the victim and pressure them into giving them access. Never give remote access of your device to an unverified person. This can lead to the scammer receiving access to any information on your computer, including personal information, sensitive client information, banking information, and more, which can have drastic consequences. If you are seeing fake pop-up error messages or ad displayed on your desktop screen, don't call the attached phone number. Legitimate error and warning messages from Microsoft never include a phone number. Additionally, reputable companies will never ask for payment in the form of gift cards or cryptocurrency. If you're unsure whether a message is real, close the window and visit the official website of the company directly to verify.
- **Debt Collection Scams:** Scammers will also pretend to be debt collectors, threatening victims with a variety of different consequences like lawsuits, arrests, FBI searches, or more to create a sense of panic and urgency within the target into thinking incoherently and falling victim to their demands. Many times, they will pressure the victims into creating a quick payment in the form of gift cards, money orders, wire

transfers, or crypto currency. It is best to cut off contact with the unknown caller and instead contact the legitimate organization for help.

- **Spoofing Caller IDs:** These scammers will use sophisticated technology to manipulate their caller ID information. Spoofing is the process of making the source of a connection appear credible, but really it is a stolen credential. To properly verify the authenticity of a call, do not solely rely on a caller ID. Be sure to cross check the caller's information and number with the official contact details from the organizations website they are posing from. If the information does not match, drop the call immediately and do not continue to engage in communication with the scammer.

- **Sweepstakes, Prize, and Lottery Scams:** Many people share a common trait: being highly motivated by the promise of large sums of money. Scammers exploit this by posing as representatives of lotteries or sweepstakes, claiming you've won a massive prize. In the excitement, they'll tell you that you need to pay a small fee to claim your winnings — but this is a scam. Legitimate lotteries will never contact you directly to inform you of a win; it's always the player's responsibility to check and report their winnings. Additionally, real lotteries do not ask winners to pay taxes or fees upfront — any applicable taxes are automatically deducted from the prize if required. Scammers often pressure victims to act quickly, urging them to send money immediately and avoid discussing it with others. If you believe you may have won a lottery, always verify through the official state lottery website or by calling their official winning numbers line.

What to do if you are being contacted by a call center scam?

- **Do Not Cave to the Pressure:** One of the most common tactics used by scammers is creating a sense of urgency to push victims into making quick, rash decisions. If an unknown or unverified person is pressuring you to send money or urging you to avoid speaking with trusted friends or family, it's a major red flag. It's important to think critically in these situations and avoid caving in. Scammers often manipulate emotions like fear, excitement, or confusion to cloud your judgement. Take time to stop, think, and consult a trusted source before proceeding.

- **Report the Number:** It's important to report the calls to the Federal Trade Commission to help contribute to the effort of removing scammers means of contacting targets. If you have disclosed personally identifiable information with a scammer, you can report it through the US Department of Justice fraud report.

- **Block the Caller:** Blocking the number of the caller will prevent them from contacting you through that number again. However, many times, scammers will try to continue contacting you through other numbers. If this happens, do not answer the phone, the less you engage with the scammer, the more likely they are to move on to a new target. If you are unwilling to engage in communication with them, they have no financially motivating reason to continue contact.

- **Join the National Do Not Call Registry:** The Federal Trade Commission has a Do Not Call Registry that will help reduce the amount of spam call you receive. This will not eliminate the chances of a scam caller from contacting you, but it does put your number on a list for telemarketers of who not to call.

What's at Stake

Anybody can fall victim to a scam. Scammers use a variety of different tactics so that they can target people of all ages, backgrounds, and demographics. It is important to have sound judgement when engaging with unknown callers or contacts and to be aware of the possibility it is a scam. If it sounds too good to be true – it probably is. Informing yourself on rising scams and cyber threats is an important step to building a strong awareness for security threats and can help prevent you or your loved ones from falling victim.