SOCIAL ENGINEERING OF EMAILS

Spam, or sending unsolicited emails, is a very successful social engineering tactic. Most spam emails that land in our inboxes is blatantly false, and this is done on purpose because the scammers who send them are looking for easy victims who lack the intelligence to spot schemes. Even though fewer individuals will open the email, those who do are more likely to fall for a scam.

In contrast to these con artists, social engineers frequently utilize spam that is designed to be difficult to detect to bypass spam filters and appear authentic. Most people are aware that they shouldn't believe emails that look to be from their company's IT department, but what about emails from odd dating sites we didn't sign up for? These emails frequently prey on our trust by pretending to be from reliable sources, and the practice of "prepending" can make matters worse.

Prepending is the process of changing the subject line of an email or adding a message that reads "RE:" or "MAILSAFE:PASSED" to the body of the message to make it seem as though: We have already been in contact with the sender; OR The email has made it past a spam filter.

When done well, this might give the unwary victim a feeling of even greater security.

Hoaxes

A fundamental component of social engineering, lying to get what you want can take many different shapes. It frequently fits with one or more of the fundamental tenets of social engineering. These lies are frequently referred to as hoaxes in social engineering. A typical hoax is to pretend to be security alerts to make the victim feel rushed. Because the alerts seem to be from legitimate sources and direct the victim to follow instructions, these phony alerts frequently abuse the victim's sense of authority and trust.

Pretexting is another type of lying employed in social engineering, in which a social engineer creates a fake justification for why a victim should divulge information or take an action.

You would probably disregard someone if they sent you an email asking for private information. On the other side, you can be duped into disclosing information to them if they claimed to be the new point of contact for a contractor working for your company.

Social Engineering and URLs

With the internet, deception is now simpler than ever, and it can happen even before a consumer visit to a website! A straightforward link to a "trusted" website can be used to deceive victims by social engineers.

When a social engineer guides people away from a trustworthy website and toward their harmful website, this tactic is referred to as pharming. Typically, this entails altering DNS data for a machine, a network, or a broader area of the internet. Making the name resolution procedure point to a different IP address enables phishing. This is frequently used to obtain banking credentials from gullible victims.

Typosquatting is another technique used to seduce unwary people into visiting harmful websites. Typosquatting is the practice of an attacker registering a domain that is strikingly like an already-existing, trustworthy website, then watching for users to access the malicious domain. For instance, a hacker might register codeAcademy.com to deceive users who are trying to access the website. A mistake as easy as mistyping or forgetting a URL could lead victims to this malicious domain.

If you're skeptical of this strategy, try finding the differences between these URLs:

kerning.com vs keming.com

google.com vs goggle.com

Identity Fraud

When an attacker utilizes a victim's personal information, it is called identity fraud. Many of us have heard of instances where dishonest individuals have pretended to be someone else to profit. Using someone else's bank account or credit card, for instance.

The purpose of identity fraud is not always financial gain. Social engineers can also use it to pose as a victim more effectively, either to deceive others or to obtain more access to the victim's accounts and resources.

On a personal level, this can involve targeting a company that the victim works for or utilizing stolen personal information to "recover" a bank account.

Larger-scale instances of this type of fraud might take the shape of invoice scams, in which an attacker modifies an invoice's details to steal money. Using social engineering to pretend to be an employee of one company and submitting false invoices to other businesses is one type of invoice scam.

If the attacker is successful, the second company won't notice the issue and will just pay the invoice.

Credential Harvesting

When an attacker obtains, or harvests, a victim's credentials, this is known as credential mining. However, credentials are frequently taken from numerous users at once, usually for financial benefit. This can be aimed at a specific person as part of a multi-stage attack.

A watering hole attack is one technique for obtaining specific credentials. An attack known as a "watering hole" occurs when an attacker gains access to a target by compromising a service, piece of software, or website used by a third party. The "watering hole" from which all the victims are "drinking" is the third-party service. This is an illustration of how shoddy security practices by third-party providers can jeopardize the safety of the companies that use them.

In 2012, a hacker gang attacked websites that supported political activism as an example of a watering hole assault. Attackers attempted to install malware on the targets' PCs by leading victims to a different infected website.

Physical Social Engineering Strategies

For an attacker, having physical access to a target opens a world of new opportunities, and often getting physical access is simpler than using technology to get in. These methods focus on getting over physical security or gaining credentials in person rather than online.

Shoulder surfing, the act of looking over someone's shoulder while they type their password is referred to as shoulder surfing. If the social engineer can do it without being discovered, this method of collecting credentials is quite effective, albeit it does require some skill on their behalf.

Dumpster diving is, as the name implies, the practice of searching through rubbish to find private information. Although it may seem absurd, this happens more frequently than you may imagine. Sensitive documents are frequently incorrectly disposed of by organizations, leaving them accessible to social engineers. This method can be used to access a variety of data, including sticky note passwords, employee data, and tax invoices. Don't forget to destroy your vital documents!

Tailgating describes the practice of following someone through a locked door before it closes. (“What? That qualifies as a cyberattack, you ask? Yes, it really can be that easy.) invoice.

Conclusion

Email social engineering is becoming frequently common and although some are obvious others are not. Many can spoof your employer’s email, legitimate institutions, or friends, family or coworkers. Telltale signs are being asked to change your password, provide any personal information, or requests for gift cards. When in doubt do not engage or responds with the email but contact the “alleged” sender for verification.