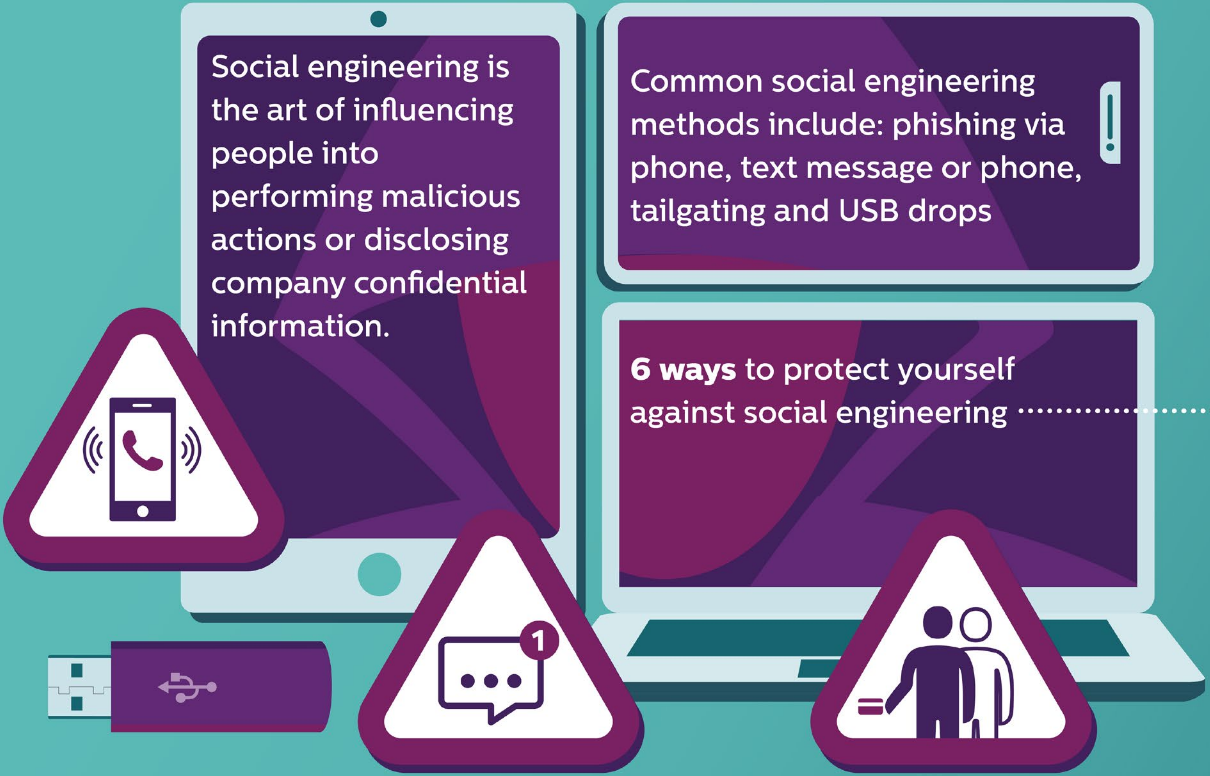
Social engineering security **best practices**

What is **Social Engineering?**



Social engineering is the art of influencing people into performing malicious actions or disclosing company confidential information.

Common social engineering methods include: phishing via phone, text message or phone, tailgating and USB drops

6 ways to protect yourself against social engineering

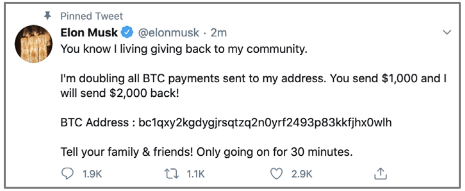
1. Don’t overshare on social media
2. Never reveal your passwords or PIN codes over the phone or by email
3. Don’t click on suspicious email links or open attachments
4. Confirm the identity of unknown callers
5. Don’t let strangers enter your workplace
6. Report suspicious emails, text messages and phone calls

Incident: Twitter users hacked

The company announced that the incident was a "coordinated social engineering attack" which targeted some of its employees with access to internal systems and tools. Some big-name accounts and dozens of others were impacted by the hack, and Twitter was unable to stop it.

1 The hack resulted in several celebrity Twitter accounts posting a message instructing followers to send Bitcoins. Twitter confirmed 130 accounts were targeted. Attackers tweeted from 45 of the accounts, accessed the direct messages of 36, and downloaded the Twitter data of seven.

2 Initially it was thought the hack was the work of professionals, but the "mastermind" was a 17-year-old from Florida. Twitter disclosed that attackers got in through social engineering, specifically through a phone spear-phishing attack, that targeted company employees.



Pinned Tweet

Elon Musk @elonmusk · 2m

You know I living giving back to my community.

I'm doubling all BTC payments sent to my address. You send $1,000 and I will send $2,000 back!

BTC Address : bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Tell your family & friends! Only going on for 30 minutes.

1.9K 1.1K 2.9K

3 Social engineering tactics were used to steal Twitter staff credentials to access an internal system to reset passwords of Twitter users. One of the hackers convinced a Twitter employee that he was a co-worker in the technology department who needed the employee's credentials to access the customer service portal.

4 While this incident raises concerns about Twitter's security practices, it also demonstrates how social engineering can be an effective tactic for hackers to use to break into a corporate network.

KEY LEARNINGS

- Never reveal your passwords or PIN codes over the phone or by email. Had the Twitter employee followed this advice, they would have avoided the hacking incident.
- Don't click on suspicious email links or open attachments.
- Report suspicious emails, text messages and phone calls
- Confirm the identity of unknown callers. Had the Twitter employee asked for an employee ID or further verification from the hacker, the hack would have been foiled.
- Don't let strangers enter your workplace: tailgating, badge surfing are commonly used by criminals to gain access into corporate offices or homes. Do not use your company email address to register on public websites, no matter how legit.
- Don't overshare on social media.