The Twitter hack dissected

By Anna Collard   24 Jul 2020

If you use the internet, you are not immune to cybercrime.

Anna Collard, MD at KnowBe4

According to Twitter statements, the incident resulted from a small number of employees being manipulated through a social engineering scheme. Twitter employees, especially those with access to administrative accounts very likely have controls such as multi-factor authentication in place. So either it was a really clever social engineering attack where the attackers not only got the employee's username and password but their one-time passwords as well, or the attackers collaborated with the employee.

Cybercriminals target people who work in key roles at major social media, offering them bribes and even go as far as threatening them and their families in exchange for account details or change of ownership of certain accounts.

Social engineers or people hackers trick us by playing on our emotions in order to suppress our critical thinking and to make us do things we normally wouldn't do. Typically, this is done via email or the phone and presented in a story that will elicit an emotional response from the victim: a low-grade form of fear, curiosity, authority, greed, or flattery. As soon as you feel your emotions being triggered, it's time to slow down and don't react.

> *They try and trigger our emotions so that we don't think critically about what is happening. It could be an email that looks like it came from the CEO saying 'I need this done urgently. Please jump on it' and because they are using an authority figure, the target is more likely to act.*

Users are also less likely to question a direction from somebody in a higher position. That is especially dangerous at the moment given the large swathes of people working from home.

Changing your passwords and applying multi-factor authentication on all your social media accounts is generally a good idea too. "We have a responsibility as an industry to make people aware. In addition to multi-factor authentication and

security protection on terminals, you have to inoculate your users to make them aware of these types of attacks because they are ultimately your last line of defence," explains Collard.

ABOUT THE AUTHOR

Anna Collard, MD at KnowBe4

For more, visit: https://www.bizcommunity.com