SecurityAdvisor

Nine Cognitive Biases Used by Hackers

Despite efforts to educate and train employees to identify phishing attempts and other malicious threats, 90% of data breaches are caused by humans. Hackers are increasingly adept at exploiting employees' fears, hopes, and cognitive biases in order to gain access to corporate data. Cognitive biases are systematic patterns that deviate from logical judgment and our brains attempting to comprehend information processing. Malicious actors can sway employees with misleading or false information by exploiting various types of cognitive biases. In order to better understand how hackers operate, follow these tips to help you and your organization better understand different methods of infiltration.

Nine Cognitive Biases:

Hyperbolic Discounting:

This bias signifies a tendency to choose immediate rewards. These rewards don't even need to be substantial. Coupons offering top consumer products for free or at steep discounts are an example of hyperbolic discounting.

Authority Bias:

This bias states that people tend to give more merit to an employee based on seniority level. For example, if an employee receives a request from their CEO to share a password or pay an invoice, they are more likely to comply.

Halo Effect:

This is the tendency for an individual to have a positive impression of a person, company, brand, product, or service. With this type of attack, a cybercriminal pretends to be a trusted entity known to the targeted individual. This is typically under the alias of a universally wellknown organization or brand, such as Apple or Google.

Habit Bias:

Attacks leveraging this bias capitalize on a settled or regular tendency or practice. An example of a malicious email using this bias could resemble a daily newsletter or report.

Optimism Bias:

This bias causes someone to overestimate the likelihood of positive events while underestimating the likelihood of negative ones. Phishing emails leveraging this bias may appear in the form of a job offer that promises a 30% pay increase.

Loss Aversion:

These attacks prey on an individual's desire to avoid losses in order to acquire equivalent gains. An example of this includes acting on an outstanding payment to avoid late fees or save credit scores.

Recency Effect:

This is the tendency to present recent information or current events that have taken place. Phishing attacks that use the allure of COVID-19 vaccinations or tax returns to entice targets are examples of this bias.

Curiosity Effect:

This suggests that humans possess an inherent desire to resolve uncertainty. When confronted with an uncertain situation, they will act to resolve it, even if expecting negative consequences. Attacks that leverage this bias might direct employees to click on malicious links under the guise of "secret offers."

Ostrich Effect:

Ils the tendency to ignore harmful information. Hackers may send emails or pop-up notifications to employees to alert of an issue or virus. Hackers then offer the user a quick fix via a link. IT departments tend to postpone patches or update reminders, so a notification like this can set in motion unintended consequences despite "good" intentions.

With a better understanding of how hackers are misleading employees through their innate cognitive biases, companies can identify these methods in action, deliver training in real-time to change behavior, and cut down on security incidents.

SecurityAdvisor

FOR MORE INFORMATION
visit **www.SecurityAdvisor.io** or email **salesleads@securityadvisor.io**