9 Cognitive Biases Hackers Exploit the Most

Bad actors have the know-how to tap into the "mental shortcuts" that are called cognitive biases and manipulate employees into compromising sensitive information or systems.

Here are examples of the top cognitive biases hackers use the most.

Hyperbolic Discounting

Choosing immediate rewards over rewards that come later in the future

ⓘ **Free coupon or special deal scams**

Habit

The tendency of users to follow recurring habits

ⓘ **Phishing emails delivered at a specific time of day**

Recency Effect

Remembering the most recent information or events best

ⓘ **Phishing attacks referencing current events**

Halo Effect

When positive impressions of a person, company, etc., influence your overall feeling of that person or company

ⓘ **Scam messages from well-known brands**

Loss Aversion

The tendency to prefer avoiding losses to acquiring equivalent gains

ⓘ **Phishing attacks threatening credit score damage**

Ostrich Effect

The tendency to avoid unpleasant information (hiding your head in the sand)

ⓘ **Phishing emails warning action should be taken quickly or else**

Authority Bias

Attributing greater accuracy to the opinion of an authority figure

ⓘ **Hackers spoofing important messages from the CEO**

Optimism Bias

Overestimating the probability of positive events while underestimating the probability of negative events

ⓘ **Phishing emails will offer fake job opportunities or insider info**

Curiosity Effect

Acting to resolve curiosity even if it could lead to negative consequences

ⓘ **Phishing attacks offering limited time offers or secret information**

Explore how a better understanding of how hackers are duping users can help you identify potential cognitive biases and deliver training that actually changes behaviors with our free whitepaper:

DOWNLOAD NOW!

KnowBe4

SecurityCoach