KnowBe4
Human error. Conquered.

9 Cognitive Biases Hackers Exploit the Most

Understanding What Makes Us Tick and Click

UNDERSTANDING WHAT MAKES US TICK AND CLICK

Human error is undoubtedly the biggest risk factor to a sound security posture for any organization. 82% of all data breaches result from human error and yet many organizations don't have a program in place to protect the human attack surface. Security teams deploy several technologies to protect their attack vectors (network, endpoints, email, web, cloud apps, etc.) but what about the human attack surface?

Despite efforts to educate and train employees to spot phishing attempts, an all-too-common horror continues. An employee in the finance department receives an email from the CEO, asking him to immediately pay a vendor invoice. The email includes an attachment of the invoice, along with the CEO's email signature. With the urgency communicated in the email, the employee pays the invoice and moves on with their day. Unfortunately, the CEO's email was spoofed.

People, no matter their tech savviness, are often duped by these scams because of their familiarity and immediacy factors.

Cybersecurity is not just a technological challenge, but increasingly a social and behavioral one.

The FBI's 2021 Internet Crime Report includes information from 847,376 complaints of suspected internet crime—a 7% increase from 2020—and reported potential losses exceeding $6.9 billion. Business email compromise (BEC) schemes, the specific form of phishing attack in the example above, were a topic complaint received in 2021. The FBI estimates BEC attacks cost $2.4 billion in 2021 alone.

Cybersecurity is not just a technological challenge, but increasingly a social and behavioral one. The top reasons cyber breaches happen point to human actions, according to Willis Towers Watson. From mistakenly disclosing account information to falling for phishing attacks, an organization's data can leak through legitimate channels and compromise its security. This social engineering easily bypasses technology barriers.

The biggest issue is that hackers have become increasingly savvy at launching specialized attacks that target specific employees by tapping into their fears, hopes, and biases to get access to their data. With a better understanding of how hackers are duping employees, companies can identify potential biases, deliver training that actually changes behaviors, and cut down on security incidents.

UNDERSTANDING COGNITIVE BIAS

Behavioral economics studies the effects of psychological, cognitive, emotional, cultural and social factors on the decisions of individuals and institutions. Behavioral economics came of age in 1970 thanks to the work of Israeli social scientists, Nobel Prize winning economist Daniel Kahneman and Amos Tversky. The understanding of cognitive psychology was revolutionized by their discovery of emotional biases. Kahneman and Tversky found significant evidence that humans, in certain circumstances, show a systematic pattern of deviation from the norm or rational judgment.

Five decades later, their research is helping companies understand why they're seeing their own employees easily fall for cyber breaches. Every day, hackers use specific cognitive biases to repeatedly target employees and leverage human cognitive biases to trick end users.

TOP 9 COGNITIVE BIASES USED BY HACKERS

To preserve cognitive resources, the human mind subconsciously takes mental shortcuts, called cognitive biases, whenever and wherever it can. While these preconceptions do not necessarily reflect reality or rationality, we rely on them to expedite and simplify information processing. These biases influence and affect not only the way we think and behave, but also our decision-making process.

Hackers tap into human cognitive biases to sway their decisions based on irrelevant or misleading information and based on false or generalized categorization.

Employees are enticed to click on fraudulent links or share sensitive company data through fake coupons or fake messages from "team managers." Here are brief descriptions of nine of the most common biases hackers exploit:

Hyperbolic Discounting

This bias refers to the inclination to choose immediate rewards over rewards that come later in the future, even when these immediate rewards are smaller.

Example: "Here's a free coupon"

Habit

This bias takes advantage of the tendency of users to follow recurring habits, building social engineering attacks around likely regular emails or other communications.

Example: "Here is your daily delivery report"

Recency Effect

This is the tendency to remember the most recently presented information best, or recent events that have taken place. Attacks like these use global events, such as the COVID-19 pandemic, to lure targets to act.

Example: "Avoid coronavirus. Click here to schedule your vaccination."

Halo Effect

This is the tendency for an individual to have a positive impression of a person, company, brand, product or service. In this type of attack, a cybercriminal pretends to be a trusted entity known to the target individual.

Example: "Message from Apple about your iTunes account"

Loss Aversion

This bias refers to an individual's tendency to prefer avoiding losses to acquiring equivalent gains. Email scams leveraging this bias urged individuals to act on an outstanding payment to avoid late fees, for example.

Example: "Act now to save your credit score"

Ostrich Effect

This bias aims to stoke fear into unsuspecting users, convincing them they've done something wrong and to take quick action to fix it, rather than tell IT and risk reprimand (sticking their heads in the sand).

Example: "You have 800 viruses. Click here to clean up your computer."

Authority Bias

This bias states that people tend to attribute a greater accuracy to the opinion of an authoritative figure. In the context of the workplace, this can include a manager, boss or CEO.

Example: "Hey it's your CEO. I need you to send me that financial information ASAP."

Optimism Bias

This bias causes someone to overestimate the probability of positive events that will happen to them and underestimate the probability of negative events. Phishing emails leveraging this bias appear in the form of job offers, for example.

Example: "A 30% pay hike is on the way. Details are in the attached document."

Curiosity Effect

Also referred to as the Pandora effect, taken from the Greek mythology of Pandora's box, research suggests that humans possess an inherent desire to resolve uncertainty. When facing something uncertain, they will act to resolve the uncertainty even if they expect negative consequences.

Example: "Here is your secret offer - click here"

SECURITY LEADERS MUST BREAK DOWN EMPLOYEES' COGNITIVE BIASES

Cybercriminals purposefully use fear, authority/hierarchy, and familiarity tactics to trick end users into clicking links or opening viral attachments. Phishing emails are highly effective today because workers have been conditioned to have an immediate response to them, particularly remote workers.

Phishing scams leverage authority bias where people tend to attribute greater accuracy to the opinion of an authoritative figure. If an employee receives a request from their CEO to share a password or pay an invoice, for example, they would be more likely to not question that request before fulfilling it.

Hackers use "recency effect bias" and "halo effect bias" to send employees emails with COVID-19 tips or tax returns from what look like legitimate global organizations, such as the World Health Organization (WHO) and IRS. These messages may have malicious content as embedded links or attachments.

Stoking our fears of compliance and security with the "ostrich effect bias," hackers send emails to employees, alerting them of a violation or viruses on their machine, and then offer a simple fix by clicking on a link. Many employees tend to postpone a patch deployment or update reminder from the IT team, so a message like this can trigger unintended consequences despite "good" intentions.

Loss aversion attacks prey on an individual's tendency to prefer avoiding losses to acquiring equivalent gains. An example of this bias in action can include acting on an outstanding payment to avoid late fees.

The impact of these biases on the business is defined by frequency and by severity. How frequently the bias is used is a strong indicator of the probability of the event occurring. Most people have received some type of phishing email based on the halo effect and hyperbolic discounting biases. Given the frequency of these types of phishing emails, there is a high likelihood that employees will fall prey to it.

The severity impact relies on human fears as the employee grants higher authority in some form to do much more harm. Granting access to their computer or transferring money in an unconventional way to comply with an urgent request may not be frequent, relatively speaking, but are often targeted. The loss to the organization is potentially more damaging with these infrequent but severe attacks.

NUDGING TOWARD A SECURE WORLD

Human biases are part of human nature, but that doesn't mean organizations can't learn from cognitive psychology and counteract these biases.

The work of Nobel Prize winner behavioral economist Richard Thaler, from the University of Chicago, shows that decision architecture and human behavior can be influenced by "subtle nudges." Based on indirect encouragement and enablement, the nudge theory offers curated choices that encourage people to make positive and helpful decisions. This reshapes existing behaviors and counteracts innate human cognitive bias.

Nudge theory, developed by Dr. BJ Fogg, is now being used effectively in cybersecurity to combat behavioral biases and help organizations obtain better defense against evolving security attacks. Humans learn and respond to in-the-moment reminders about behaving securely. One of the most common and best examples is the use of a password strength meter. As someone chooses a password, the longer and more complex it becomes, the more a bar fills up or a sad face turns into a smiley face.

6 STEPS FOR A BUILDING A STRONG SECURITY CULTURE

Across the organization, people need to understand the fundamentals of making the most secure cyber decisions and what's expected from them in complying with security policies. Cybersecurity awareness training introduces the workforce to the organization's security policies, the most prevalent cyber threats, best practices for behaving securely, and how to reach someone for help with cybersecurity matters.

A comprehensive, personalized employee security awareness program, including education, training and assessment can be a game-changer in improving an organization's security culture.

1. Educate the entire organization on cybersecurity basics and roles
2. Provide relevant on-demand training and real-time contextual security tips
3. Customize training to specific role requirements
4. Run frequent simulated phishing attacks to keep everyone on their toes
5. Use AI and data analysis to target content for high-risk users
6. Measure and report the results

REDUCE SECURITY INCIDENTS AND CHANGE BEHAVIOR THROUGH HUMAN RISK MANAGEMENT

Human behavioral research suggests that people are more motivated and more likely to adopt a new behavior when given small tasks and immediate small rewards. This is even more true in cybersecurity. For better retention of the training, the content needs to be engaging, relevant, quick and frequent.

Basic psychological studies have also shown that long-term behavior change is derived from consistent training and engagement. Providing constant reminders to apply knowledge at the right moment is the best way to facilitate individual changes in employees' behavior. To start building a strong security culture, organizations should constantly communicate educational content on new and emerging threats to employees in real-time to prevent breaches. Ensuring employees receive personalized coaching and guidance based on their aptitude, susceptibility to threats, job role, and department is an effective way to ultimately improve an organization's overall security posture.

Your best defense is to develop a strong security culture across your organization that engages your users and reinforces the importance of following your organization's security policies, strengthening your human firewall. Your IT and security operations center (SOC) teams play a critical role in strengthening your overall cybersecurity posture.

SecurityCoach unites these two teams with a shared goal: strengthen the human firewall to further improve your security culture and reduce cybersecurity risk. SecurityCoach helps you augment your security awareness training effectiveness and take a data-driven approach to quantifying and reducing human risk by combining existing technology with real-time behavior coaching and new-school security awareness training.

SecurityCoach is natively integrated with KnowBe4's new-school security awareness training platform and is the first real-time security coaching product created to help IT and SOC teams further protect your organization's largest attack surface — your employees.

With SecurityCoach, you can gain additional value from your existing security stack by integrating with security vendors you already use. Based on alerts generated by your organization's security products, SecurityCoach analyzes and identifies detected threat events to send your users real-time coaching SecurityTips at the moment risky behavior occurs. When you provide instant coaching on risky activities, you reinforce your security awareness training and policies, improve knowledge retention and help your users understand the risks associated with their behaviors. You are also able to build a more effective and mature security culture across your whole organization in less time.

Learn More About **SecurityCoach**

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01D01K01