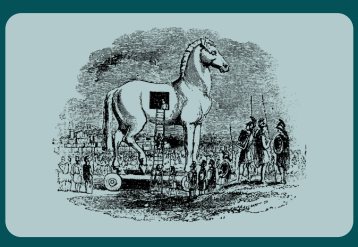
Elevate Security

The Rise of Social Engineering Attacks: An Overview of the State of Cybercrime

Social engineering attacks focus on human interactions with the goal of influencing workforce users to break security protocol and essentially give up unfettered access to a company's systems, networks, and/or source code. These attacks are growing more sophisticated every day, victimizing your workforce users and triggering security breaches. The worst part? Social engineering attacks are on the rise.

A History of Social Engineering Attacks



1184 B.C.E. (Yes, really)

The Trojan Horse Attack at the Battle of Troy

The Greeks social engineered their way into the gates of Troy by tricking the Trojans into believing the wooden horse was a peace offering. When in reality, Greek soldiers were hiding inside, waiting to attack the Trojans once they breached the city's gates.

The 20th Century

Kevin Mitnick's Social Engineering Attacks

Mitnick, now a leader in cybersecurity, is notoriously known for his various computer and communications-related crimes which he performed via social engineering. His cyberattacks focused on fostering relationships with employees at designated companies to coax proprietary information out of them.

The 21st Century

Recent Social Engineering Attacks on IT Engineers and Developers

During 2022, enterprises including a ride share app, a password manager platform, and a video game publisher have all been victimized by social engineering attacks. If these social engineering attacks are impacting major corporations and large enterprises, your organization could be at risk as well.

Social Engineering's Latest Victims: IT Engineers and Developers

While any workforce user can become a target of a social engineering attack, today, software engineers are among the most targeted.

Why attack engineers and developers?
Gaining access to application code gives attackers maximum leverage and the ability to inject backdoors for long-term persistence.

Since April 2022, social engineering attacks on IT engineers and developers have increased
142%!

In July 2022, IT engineers were targeted
8x more often
than non-engineers.

In August 2022, IT engineers were targeted
6.8x more often
than non-engineers.

Since April 2022, social engineering attacks on IT engineers, on average, have
increased 1.42x
from 5.79 times per month to 8.25 times per month.

In Summary

Elevate research determines that IT engineers and developers are being attacked more often than other organizational departments. Although engineers are not inherently riskier than other workforce users, **this increased frequency of attacks raises their likelihood of unintentionally triggering a security breach, regardless of their behavior.** In turn, an engineer's level of insider risk is something security leaders should be aware of and monitor on a regular basis.

Our research determines:

There's no significant difference between overall risk scores for engineers vs. non-engineers.

There is a significant difference in attack rates between engineers vs. non-engineers after July 2021.

There is an upward trend in attack rates for engineers, which accelerated starting around April 2022.

Since engineers (and other workforce users) are being tricked and victimized by social engineering attacks, organizations need a way to understand and mitigate user risk at an individual level. **With Elevate Security, you can identify and respond proactively to your organization's highest risk users to prevent social engineering attacks (among others) from affecting your engineers and your organization as a whole.**

Get in touch with us to learn more about how Elevate Security can help protect your organization from the inside out.

About Elevate Security

Elevate Security is a comprehensive workforce cyber risk monitoring, management, and mitigation platform that identifies and responds proactively to your organization's highest risk users. With deep visibility into each individual's user risk level, including the actions they take and the frequency they are attacked, Elevate Security provides security teams with the visibility and risk scoring necessary to zero in on the most likely source of the next security incident, and stop it before it starts.

For more information, please visit elevatesecurity.com.