The Permission Paradox

Cybersecurity can't read minds. But it can map vulnerabilities. Discover how at cpf3.org

save for later

What if the very culture of respect and efficiency you've built is the vulnerability a hacker is banking on?

Swipe next ⟶

follow for more

Unquestioning Compliance with Apparent Authority

The automatic tendency to obey instructions from someone perceived to be in charge, without critical evaluation.

(Milgram, 1974)

Swipe next ⟶

save for later

The Logical Flaw:

It’s like stopping your car at a green light because the car in front of you has its brake lights on. You’re following the immediate signal, not the actual rule.

Swipe next ⟶

save for later

Primary Attack Vector: CEO Fraud / Business Email Compromise (BEC)

An attacker impersonates a high-level executive (the authority) via email and weaponizes this bias by issuing an urgent, unusual financial request that bypasses normal security protocols because it feels legitimate.

Swipe next ⟶

The Attack

Case: Ubiquiti Networks (2021)
An employee received emails from an impersonated executive and lawyer, leading to a wire transfer of $46.7 million.

Consequence: Major financial loss.

Search: "Ubiquiti CEO Fraud"

save for later

The Solution

Awareness training fails because this is a pre-cognitive, automatic response. You need a structural solution.

The Cybersecurity Psychology Framework (**CPF**) maps this vulnerability through indicators like:

CPF Indicators 1.1, 1.6, 1.8

Swipe next ⟶

save for later

The Cybersecurity Psychology Framework (CPF). Open Source on GitHub. Professional certifications & audits available.

For CISOs, security leaders & auditors: Map your human terrain.

Cybersecurity can't read minds. But it can map vulnerabilities. Discover how at cpf3.org