The Impostor Directive

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

What if the very hierarchy that makes your company efficient is also its greatest security vulnerability?

Swipe next →

follow for more

Obedience to Authority

The psychological tendency to comply with instructions from a perceived authority figure, even if they conflict with one’s personal conscience or security protocols.

(Milgram, 1974)

Swipe next ⟶

save for later

The Flaw

It’s like a fire drill: if the person in charge says, “Don’t worry, it’s a test,” you stay at your desk, even if you smell smoke. You outsource your judgment.

Swipe next ⟶

save for later 🔖

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

Attackers impersonate an executive (the authority) to create urgency and bypass verification. The bias makes the request feel legitimate.

Swipe next ⟶

The Attack

Case: Ubiquiti Networks, 2015.

Fake CEO email instructed a junior employee to transfer $46.7 million to a fraudulent account.

Consequence: Major financial loss.

Search: "Ubiquiti CEO fraud"

Swipe next ⟶

save for later 🔖

The Solution

Awareness training fails because the compliance is pre-cognitive; it happens before logic kicks in. The solution is structural.

The **Cybersecurity Psychology Framework** (CPF) maps this vulnerability through indicators like **1.3** (Authority Impersonation Susceptibility) and **1.6** (Authority Gradient Inhibiting Reporting).

Swipe next ⟶

follow for more

The Cybersecurity Psychology Framework (CPF).

Open Source on GitHub.

Professional certifications & audits available.

Discover at cpf3.org