

Security by Culture

Why Awareness Matters More Than
Tools

INNOVATE. INTEGRATE. EXCEED.



inovex



Hello,

I am Christoph Menzel

Head of Security Excellence, Location Erlangen

- Software developer by heart
- Working in the IT sector since 2004
- Security from Technical, Strategic, and Business perspectives
- Speaker, Trainer, Coach and Author

 christoph.menzel@inovex.de

 [@christoph-menzel](#)

 [@traveling-developer](#)

 [@traveling_developer_42](#)

 [@traveling_developer](#)

95% of all data breaches are caused by
human error

(mimecast - The State of Human Risk 2025)

POLARA

(April 2025)

- US manufacturer of acoustic pedestrian signal systems (APS)
- Pedestrian signals manipulated in several major US cities
- Normal announcements replaced with celebrity voices:
 - Jeff Bezos
 - Elon Musk
 - Mark Zuckerberg
- Service app freely accessible in App Stores (iOS & Android)
- Standard password (1234) publicly visible on the internet



McDonald's Application Portal (July 2025)

- McHire.com, operated by the US company Paradox.ai
- AI bot „Olivia“
 - Collects personal information
 - Analyzes personality traits
- Sensitive data of over 64 million people stored
- Admin access via:
 - Username: 123456
 - Password: 123456



Microsoft Entra ID (July 2025)

- Microsoft's identity and access management service
- All Entra ID tenants worldwide potentially affected
- CVSS score: 10 out of 10 (maximum criticality)
- Insufficient token validation in the Azure AD Graph API
- Enabled full access to external Entra ID tenants
- No traces in logs due to the use of actor tokens

Louvre

(October 2025)

- World's most visited museum & home to French Crown Jewels
- 9 pieces of royal jewelry stolen in under 7 minutes
- Security audit warnings ignored for 10+ years
- Only 39% of galleries covered by cameras
- CCTV surveillance password: "LOUVRE"
- Security vendor Thales software password: "THALES"



Carlsberg

(January 2026)

- Visitor experience platform for the interactive exhibition in Copenhagen
- QR-code wristband IDs link visitors to personal photos & videos
- Full brute-force of all IDs possible in ~52 hours from a single laptop
- No effective rate limiting
- Videos & photos of all visitors publicly accessible
- Responsible Disclosure ignored for 150+ days



Facts and Figures

The human factor in security incidents

- **32%** Misuse of access data (e.g. reused passwords)
- **23%** Social engineering attacks (e.g. phishing)
- **14%** Unintentional errors (e.g. misconfigurations)
- **7%** Interaction with malware (e.g. opening infected attachments)

(Source: Verizon, 2025 Data Breach Investigations Report; n=10.798)

Exposed Secrets in Public Repositories

- **39%** Web Application Infrastructure (e.g. Authentication Tokens)
- **32%** Development Environment and CI/CD (e.g. GitLab Tokens)
- **15%** Cloud Infrastructure (e.g. API Keys)
- **5%** Databases (e.g. Connection String)
- **5%** Other (e.g. SSH Keys)

(Source: Verizon, 2025 Data Breach Investigations Report; n=441.780)

The most common entry points in security incidents

- **34%** Web application (e.g. SQL injection)
- **27%** Email (e.g. phishing attacks)
- **21%** Carelessness (e.g. development errors)
- **18%** Direct installation (e.g. ransomware)
- **13%** Desktop sharing software (e.g. TeamViewer)
- ...

Password Management

	Home	Work
Memory	54%	53%
Pen & Paper	33%	34%
Password Management Software	32%	30%
Digital Documents	20%	18%
Email	16%	9%
Other	3%	5%

Why Tools Alone Will Not Save Us

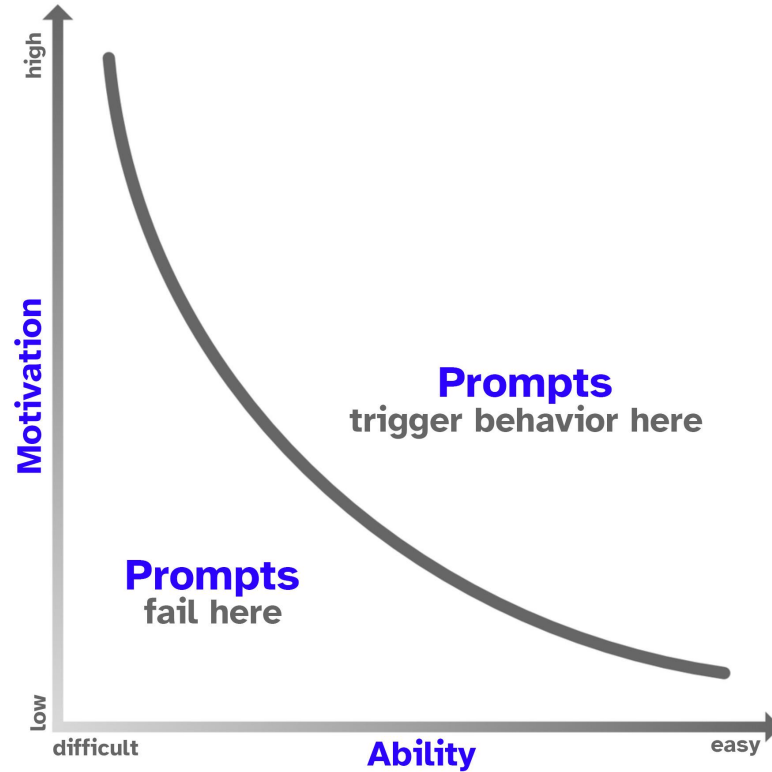
- Every breach we just looked at certainly had tools in place
- The failure was never the tool, it was the decision around the tool
 - Who set the password
 - Who skipped the audit
 - Who ignored the disclosure for 150 days
- Tools defend against known attacks. Culture defends against everyday decisions.
- Security is the sum of thousands of small choices
 - And those choices are shaped by culture, not by software

Change Behavior. Build Culture.

Fogg Behavior Model

- Behavior is the result of three factors (B=MAP)
 - Motivation
 - Am I sufficiently motivated to perform the desired action?
 - Do I feel addressed?
 - Do I feel responsible?
 - Ability
 - Do I have the opportunity to do something?
 - Do I have the necessary and correct skills / knowledge?
 - Prompt / Trigger
 - Is there a prompt?
 - Is the environment designed accordingly?

Fogg Behavior Model



Fogg Behavior Model - First Example

Reporting a suspicious email

- Motivation
 - Low, "not my job" or "probably nothing"
- Ability
 - Low, no clear process, who do I even tell?
- Prompt / Trigger
 - The suspicious email itself

→ **Prompt fails**

Fogg Behavior Model - Second Example

Reporting a suspicious email (done right)

- Motivation
 - High, the team / company celebrates reports, even false alarms
- Ability
 - High, one button in the email client, no form, no questions
- Prompt / Trigger
 - The suspicious email itself

→ **Prompt triggers behavior**

Leadership Sets the Tone

- Managers must lead by example
 - Commitment in actions, not just in language
 - Culture is not created by posters on the wall
- Create psychological safety
 - Reporting an incident must be easier than hiding one
- Practice trust, transparency, and openness
- Security is not just an IT topic

Champions Carry the Culture

- Identify Security Champions in every team
 - Voluntary, not assigned. With time officially allocated
 - Present it as a career path, not extra work
- Give security a recognizable identity
 - Mascots, slogans, real stories beat corporate phrases
- Make learning continuous and low-friction
 - Capture the Flag events, Lunch & Learn, internal community

Make the Secure Way the Easy Way

- Developer experience is a security feature
 - Frustrated people seek workarounds. Every time.
- Integrate security into the daily flow
 - IDE plugins. CI/CD security gates. Secrets-Manager by default
- Remove bureaucratic hurdles
 - For training, for reporting, for asking questions
- If your secure way is harder than the workaround, you have already lost

What Good Looks Like

Netflix: "Paved Roads" instead of policies

- Security team builds secure-by-default platforms for auth, secrets, certs
- Developers stay on the road by choice, not by mandate
- Cultural foundation: "Context, not control"
- The fastest path to production is also the most secure
- Result: security scales without slowing engineering down
- Similar approaches: Spotify ("Golden Path"), GitLab (public Security Handbook)

What's One Conversation Worth Having?

- About leadership
 - Where in our company do words on security not match actions?
- About process
 - Which security workaround do we all quietly use?
- About people
 - Who in our team would make a great Security Champion if we just asked?

Tools Buy You Time. Culture Buys You Resilience.

- The next breach in your company will not be caused by a missing tool
- It will be caused by a decision someone made
 - Under pressure
 - Without context
 - Without backup

Let's live security, not just talk about it.

Thank you!

