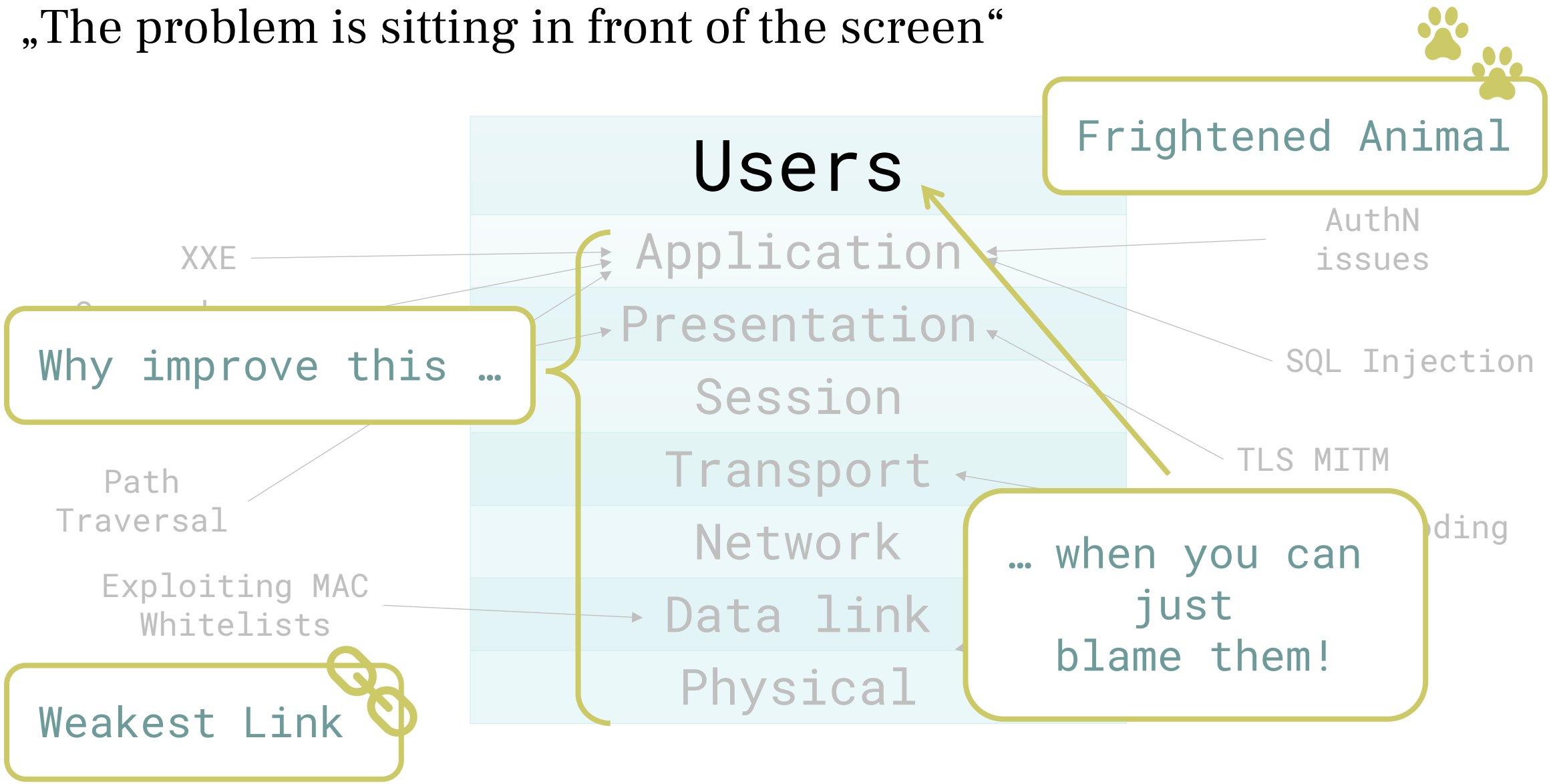
The Human Factor

Cybersecurity's weakest link or most adaptive defense?

Public

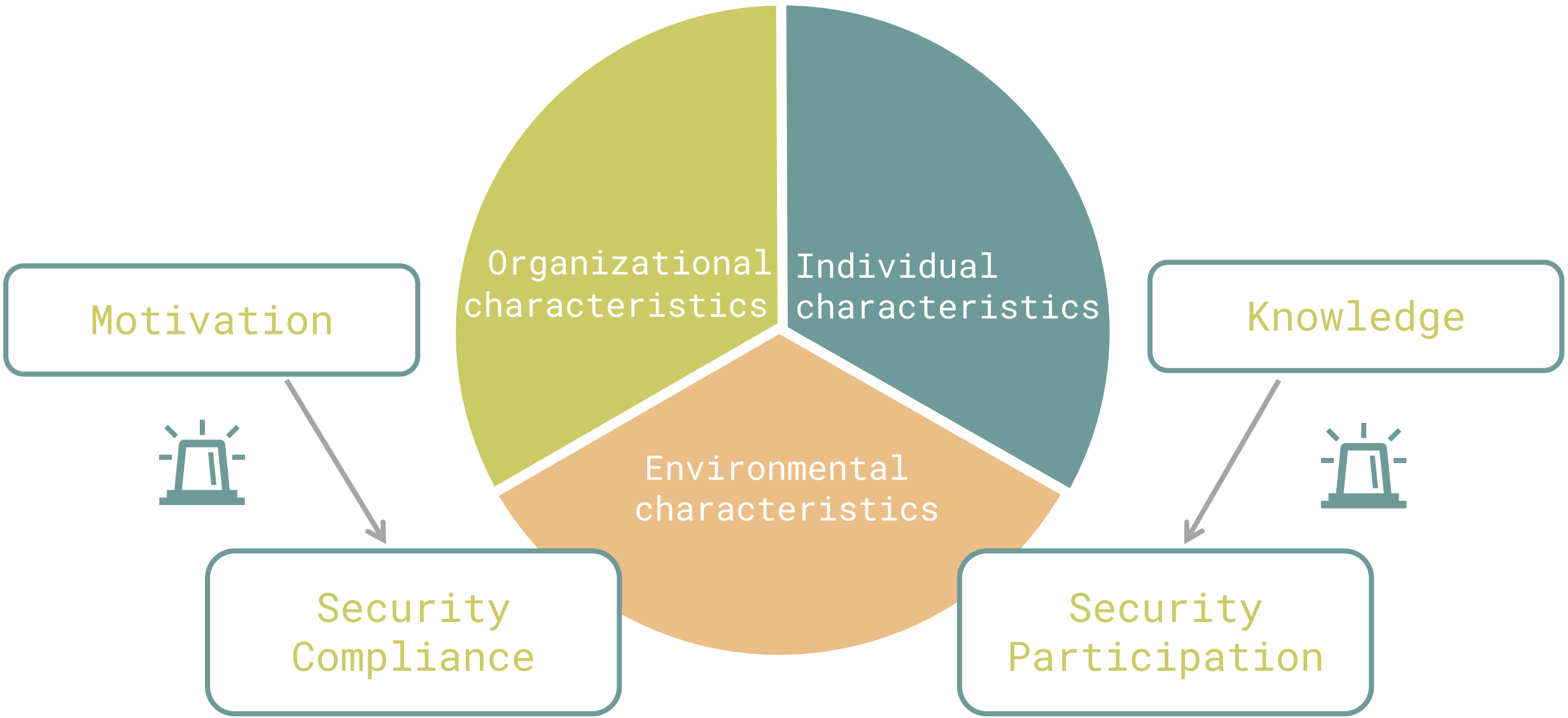
CERTITUDE

„The problem is sitting in front of the screen“



Assumptions [Soliman & Järveläinen]

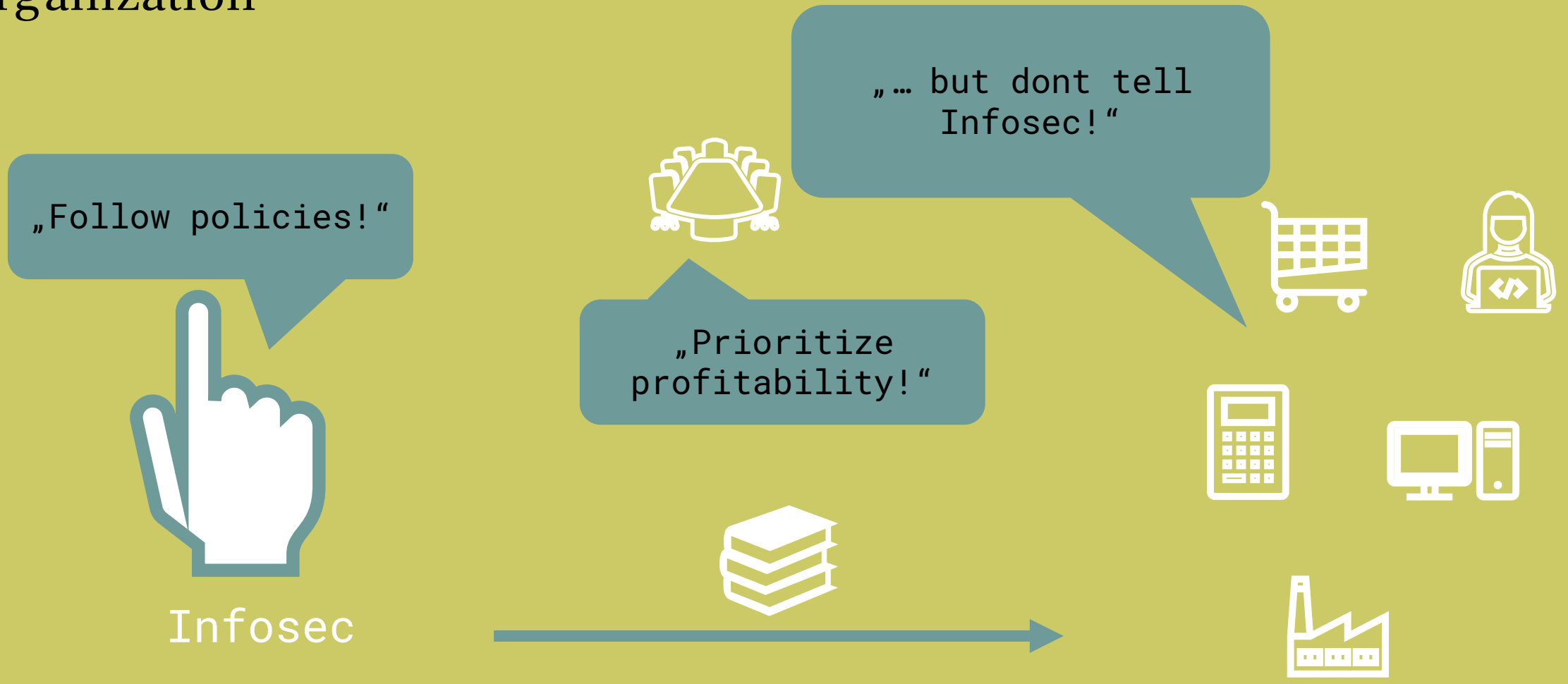
Security Behavior in Organizations



People don’t fail randomly. They fail predictably within the system we design.

- **Security Climate/Culture**
- Security Trainings
- Security Policies
- Social Systems
- Usability
- (Dis-)Incentives
- …

Organization



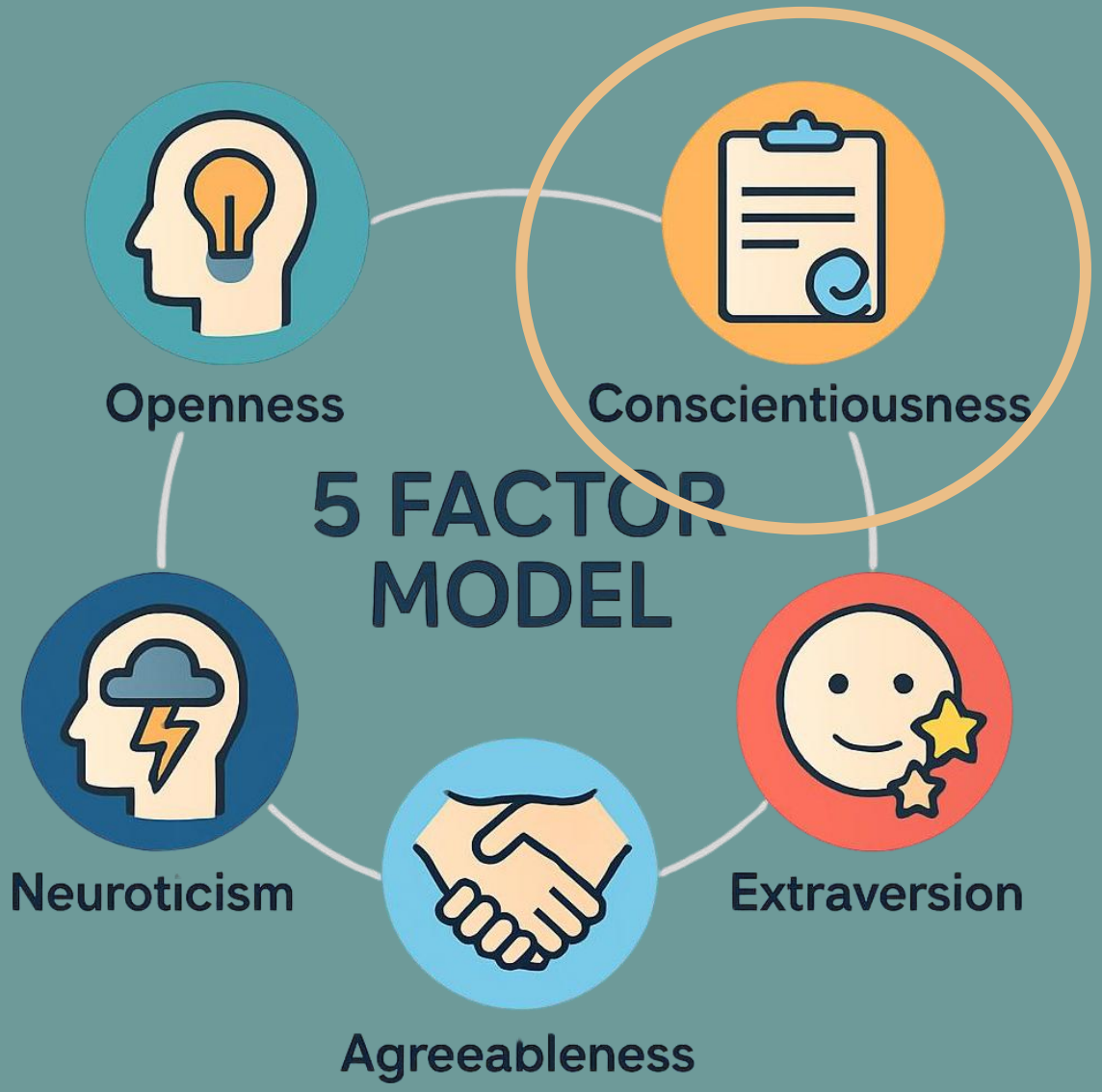
Environment

Job Pressure

Security Event

Workgroup

Five Factor Model (FFM) – BIG 5

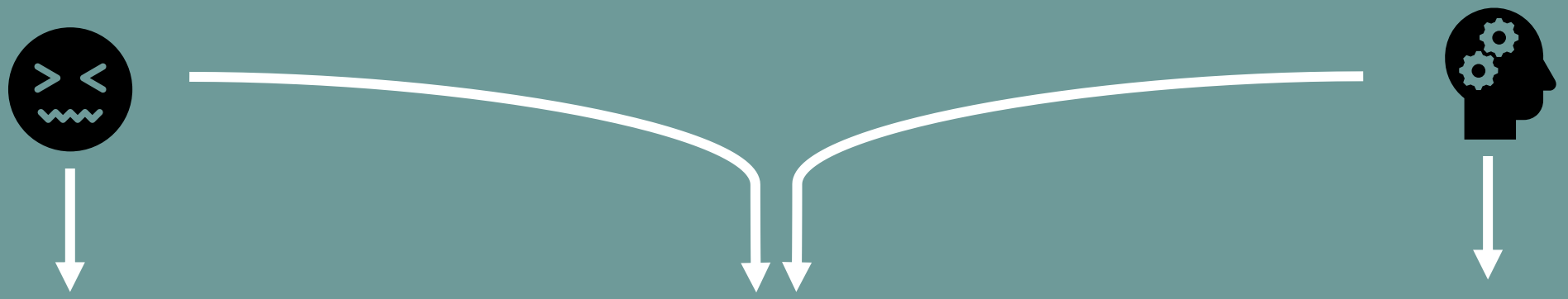


Other relevant personality traits

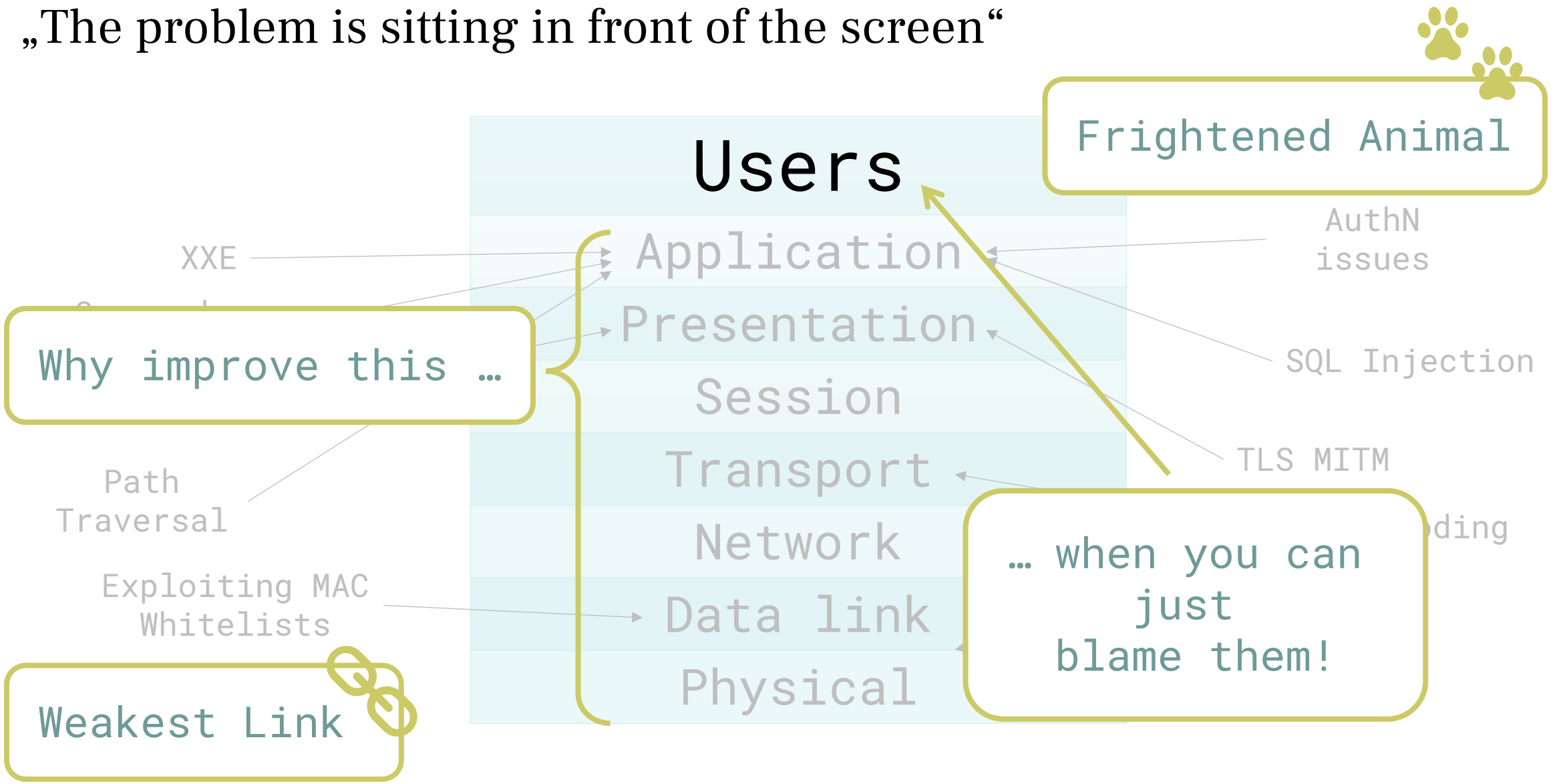
> Locus of control
> Propensity for risk-taking
> Job attitudes
> Safety attitudes

Individual Human Behavior

~~If people know better, they will act better~~



„The problem is sitting in front of the screen“



Recommendations

Design organizations for collaboration / align the organization

- bridging = break silos
- shared responsibility: community over control
- security = team sport
- foster collaboration
- empower security teams
- reward good behavior
- …

Design for individuals

- balancing awareness + confidence
- motivation > fear
- enable action
- support decision-making
- Frame the human as an asset ->„security hero“: sensors, adaptive defenders
- …

Design environments for secure behavior

- adopt security by design
- reduce cognitive and workload pressure
- focus on motivation, not just training
- …

Systems Designed for Humans to Fail

Why does security not work in practice

„Policies are made to pass audits – not actually for you to follow“

1. Passwords must be 14 characters long, contain uppercase, lowercase, special and number characters
2. Don‘t re-use passwords
3. Don‘t re-use private passwords for company accounts
4. Passwords need to be changed at a minimum every 30 days

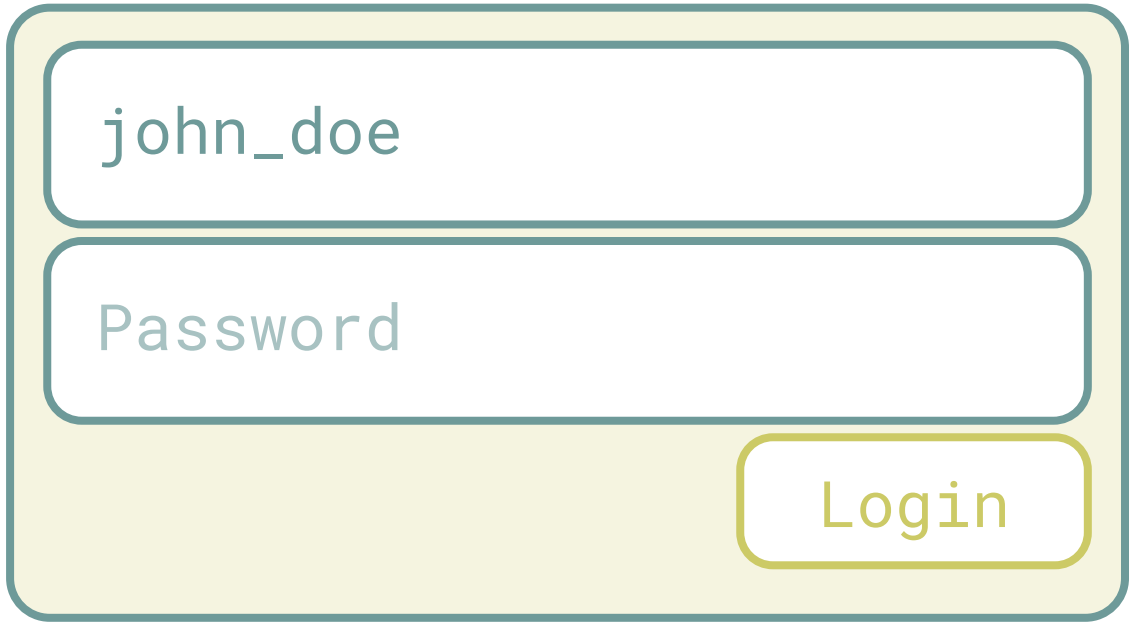
```
COMPANY: NEXT CHANGE: 2026-06-01
PRE-BOOT AUTHENTICATION: **************
AD:                      **************
PASSWORD MANAGER:        **************
PHONE UNLOCK PW:         **************
VISA PIN:                ****
SIM PIN:                 ******

PRIVATE:
PASSWORD MANAGER:        **************
WINDOWS LOGIN:           **************
PHONE UNLOCK PIN:        ******
GARAGE DOOR PIN:         ******
VISA PIN:                ****
AMEX PIN:                ****
```

Passwords

1. We know passwords are insecure
2. Majority of authentication is based on passwords
3. ???
4. Why are so many accounts breached?

Force of Habit

When a user is inactive for over 10 minutes, they must be forced to re-authenticate.

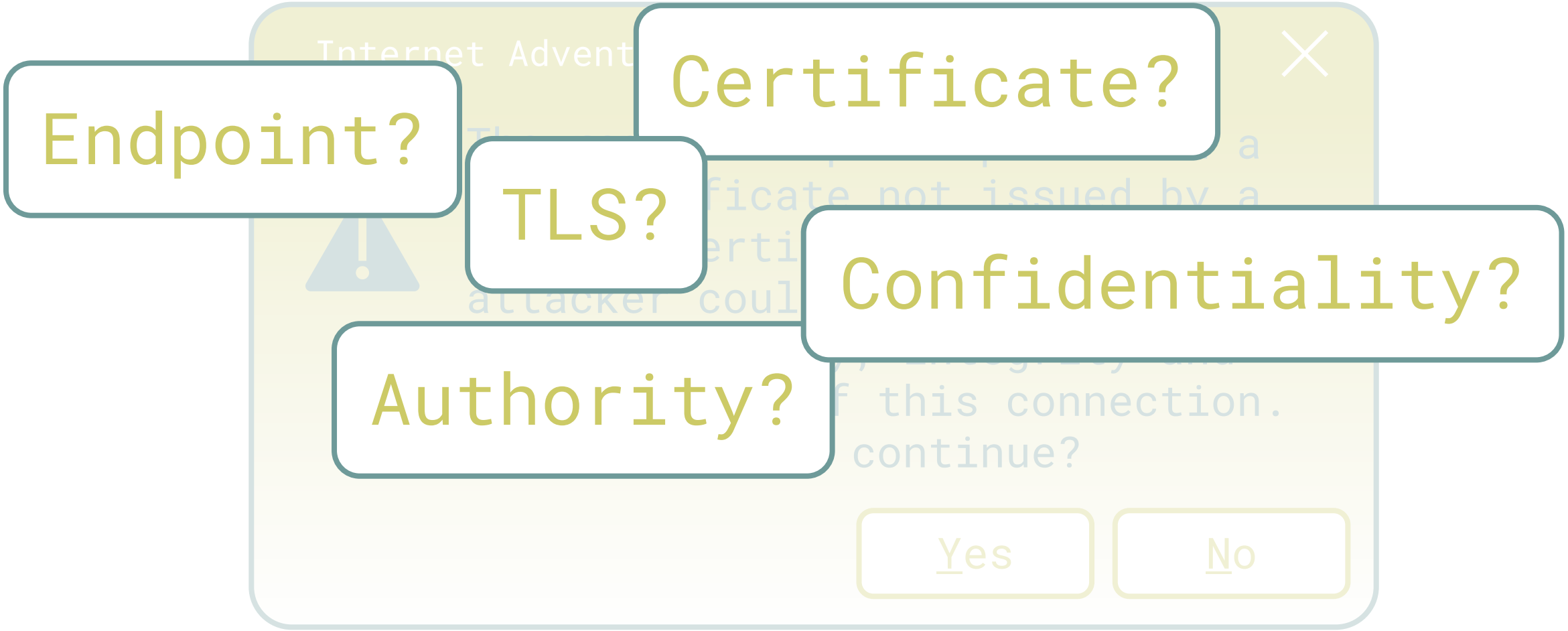


Alert Fatigue

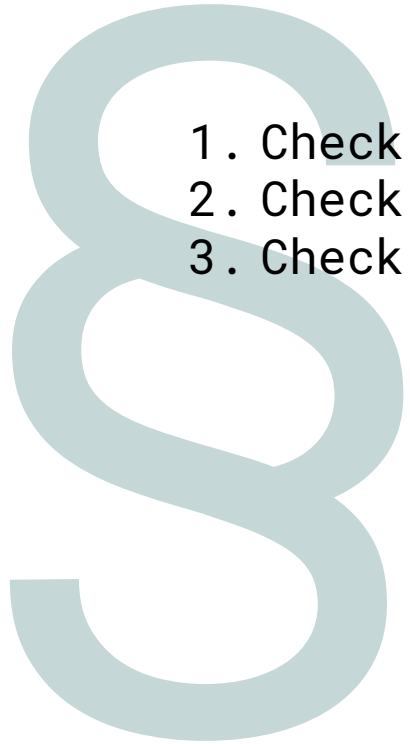
Source: Cstutz
(CC BY-SA 4.0)
Wikimedia Commons

CERTITUDE

Principal of Psychological Acceptability [Saltzer & Schroeder]



Psychological Acceptability: Phishing

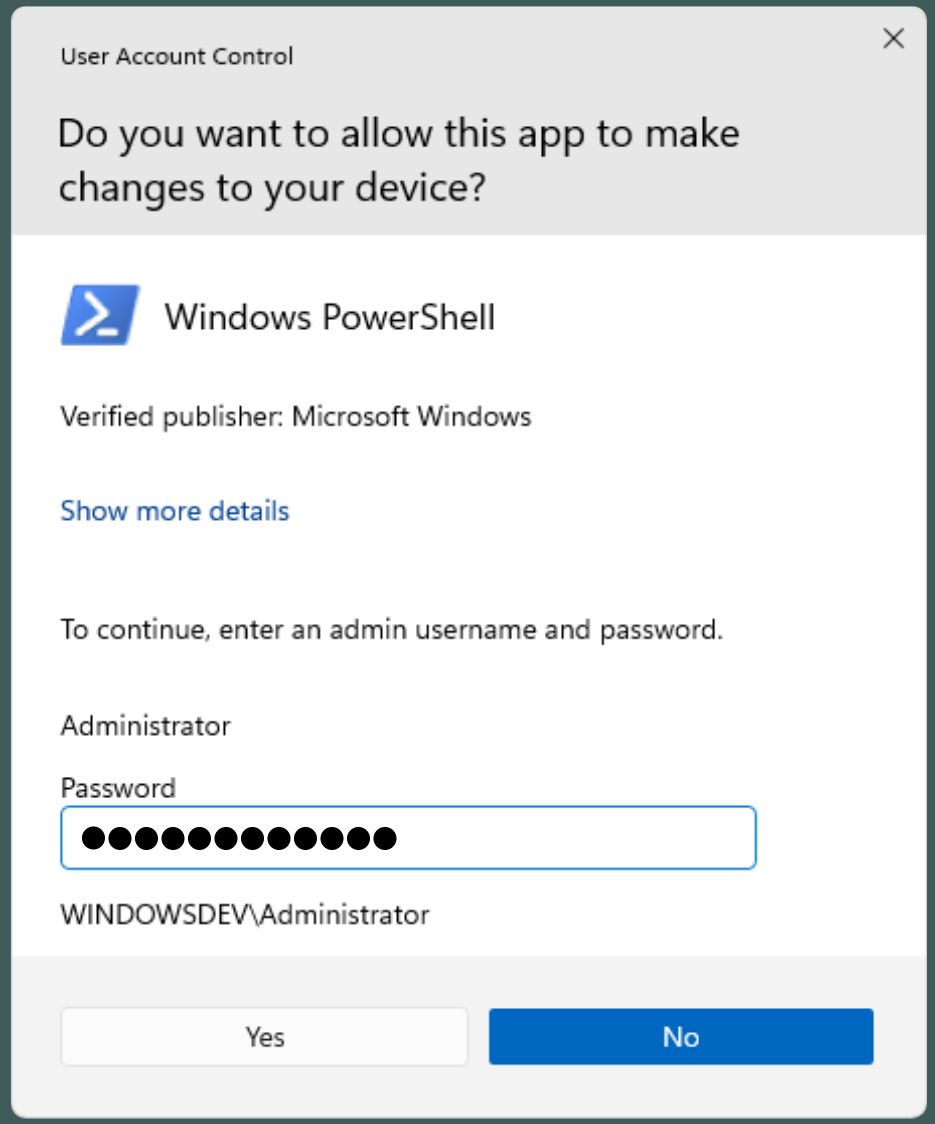


1. Check Sender
2. Check Hyperlinks
3. Check URL

```
https://eur01.safelinks.protection.outlook.com/...
https://microsoft.com@example.com/login.php
```

Spot the phishing domain:

```
microsoftonline.com
office.com
cloud.microsoft
microsoft.com
teams.com
microsoft-online.com
sharepoint.com
outlook.com
```


User Account Control
Do you want to allow this app to make changes to your device?
Windows PowerShell
Verified publisher: Microsoft Windows
Show more details
To continue, enter an admin username and password.
Administrator
Password
WINDOWSDEV\Administrator
Yes
No

Secure Layer 8 Design

> Who are your users?
> What can you **really** expect from your users?
> Why did users fail?

Human Intrusion Detectors

Key Takeaways

1. Humans are more **complex** than fear-driven actors
2. Security is a **complex socio-technical system**
3. Humans are not just users
4. Cybersecurity fails, because we **frame humans incorrectly**
5. Cybersecurity is not solved by fear or trainings alone
6. Cybersecurity success depends on alignment between the security team and the organization
7. Cybersecurity not as a compliance issue but a **system design problem:** Well-designed systems enable better human decisions

Better metaphors → better systems → better security

Q & A

Web https://certitude.consulting/

LinkedIn certitude-consulting

Sources

[Saltzer & Schroeder]
The Protection of Information in Computer Systems (JEROME H. SALTZER, MICHAEL D. SCHROEDER)
https://web.mit.edu/Saltzer/www/publications/protection/

The Line of Death
https://textslashplain.com/2017/01/14/the-line-of-death/

[Soliman & Järveläinen]
Reconceptualizing the Human in the Loop: A Problematization of Taken-for-Granted Metaphors in Cybersecurity Research

[Galletta et al.]
Balancing Fear and Confidence: A Strategic Approach to Mitigating Human Risk in Cybersecurity.

[Durcikova et al.]
United we stand, divided we fall: an autogenic perspective on empowering cybersecurity in organizations.

[Dennis]
Employees are not the weakest link: an occupational safety view of information security.

If most of your users are “too dumb” it's a YOU-problem.

The human is not the weakest link. A badly designed system – and a disconnected organization is!