Evaluating Human Awareness in Red Teaming Exercises

Who am I

Kaspar Jüristo – Head of Offensive Security Team

Penetration Testing and Red Teaming

15 years of experience in IT

Last 8 years specializing in cybersecurity.

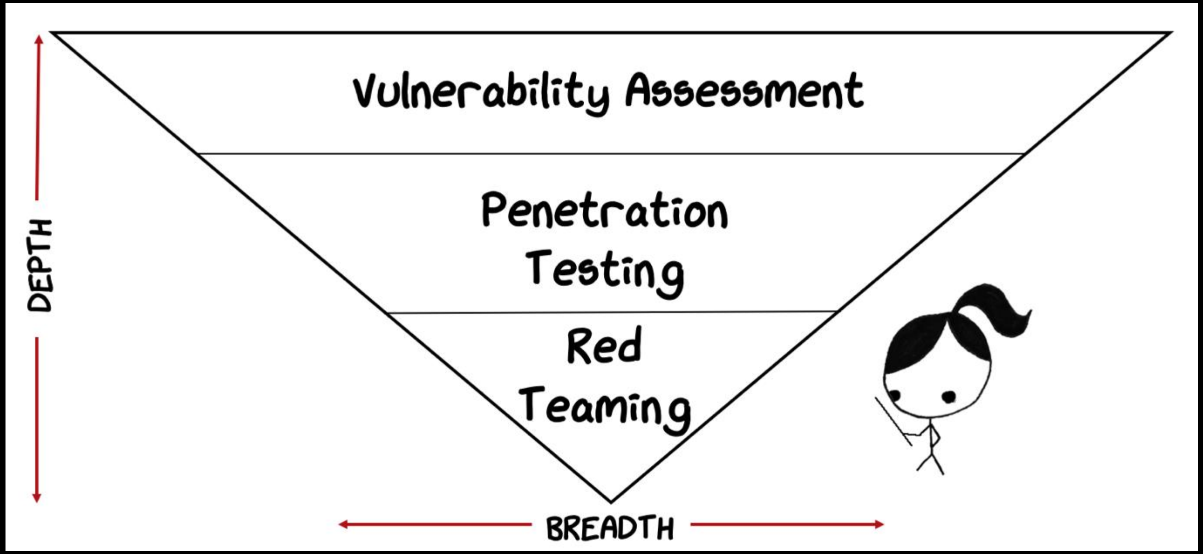
Focusing on offensive security activities past 5 years.

Master's thesis topic "How to Conduct Email Phishing Experiments“

What is Red Teaming?

Purpose: Identifying weaknesses and vulnerabilities, including human factors.

- Prepare for real cyber attack
- Get a realistic assessment
- Remediation steps with priority
- Justify investments in security



https://threatexpress.com/redteaming/red_vs_pen_vs_vuln/

Importance of Human Awareness

Stanford Research: 88% Of Data Breaches Are Caused By Human Error

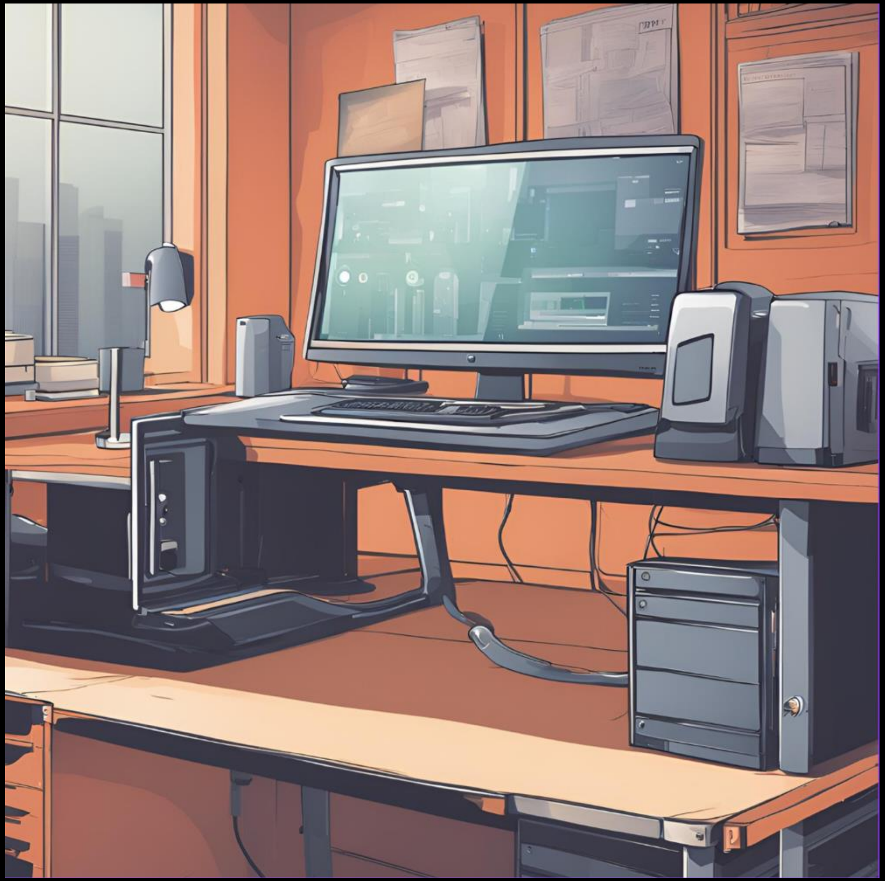
- **Tactics:** Social engineering
- **Prevention:** educating people
- **Promoting Skepticism:** less likely to trust unsolicited requests
- **Security Culture:** Regular training and updates on evolving threats

How to change Human behaviour?

Example Case #1 – Unlocked Computer

Cake emails

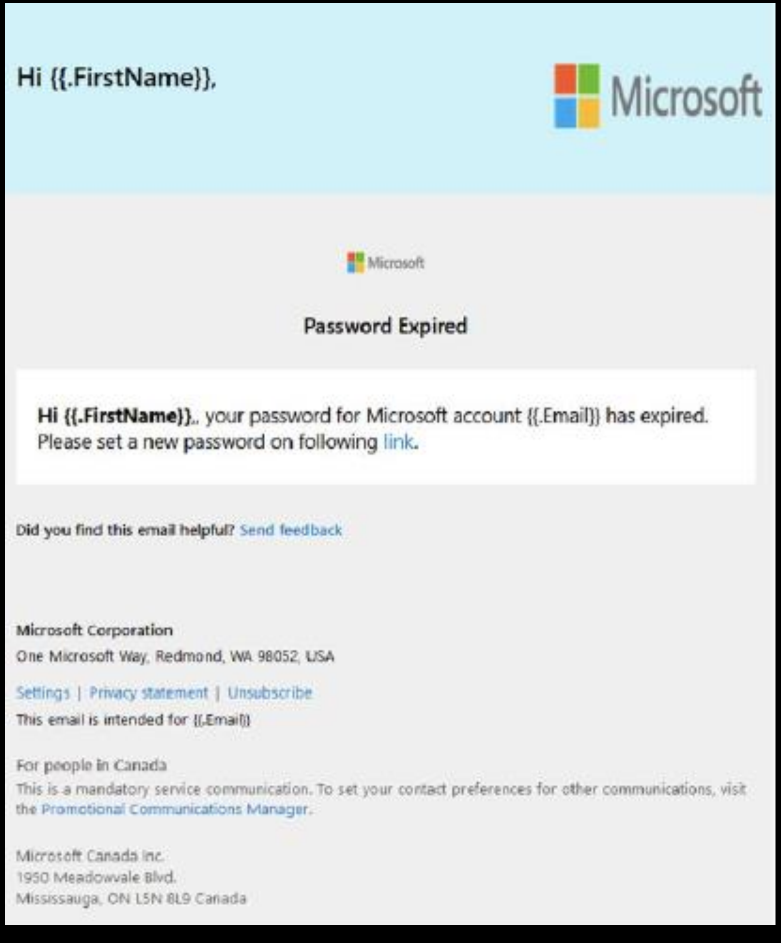
- Before Execution
  - Visual enumeration
- Execution
  - Physical access was only restricted with curtains.
  - Employees came to ask about our work ID
  - Password file on the desktop ☺
  - Active session to internal services



Example Case #2 – Phishing

Microsoft Password Expired

- Before Execution
  - Similar domain
  - Landing page and email
- Execution
  - Low number of creds
  - CEO spoofing as second email
  - Very high number of creds ☺



Hi {{.FirstName}},

Password Expired

Hi {{.FirstName}},, your password for Microsoft account {{.Email}} has expired. Please set a new password on following link.

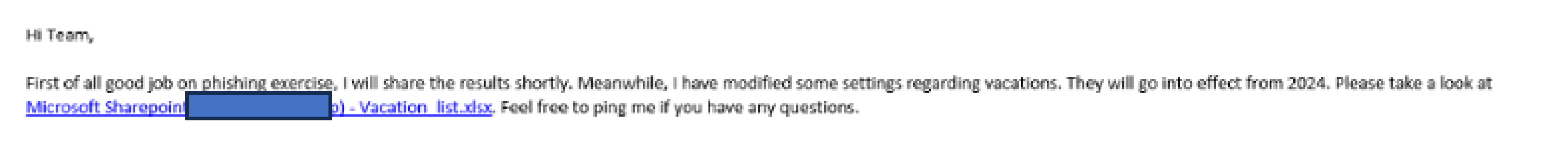
Did you find this email helpful? Send feedback

Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA

Settings | Privacy statement | Unsubscribe
This email is intended for {{.Email}}

For people in Canada
This is a mandatory service communication. To set your contact preferences for other communications, visit the Promotional Communications Manager.

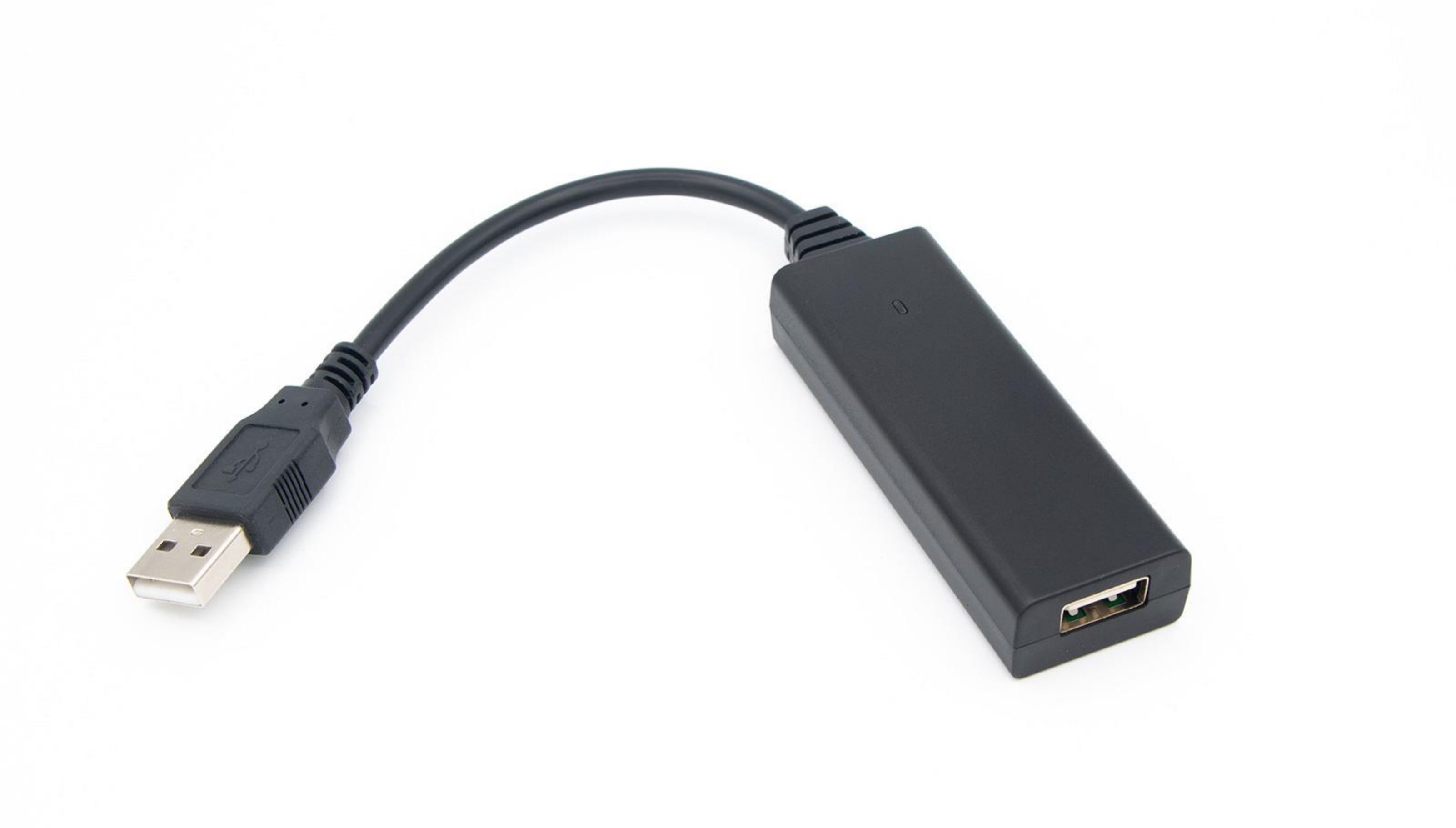
Microsoft Canada Inc.
1950 Meadowvale Blvd.
Mississauga, ON L5N 8L9 Canada



Hi Team,

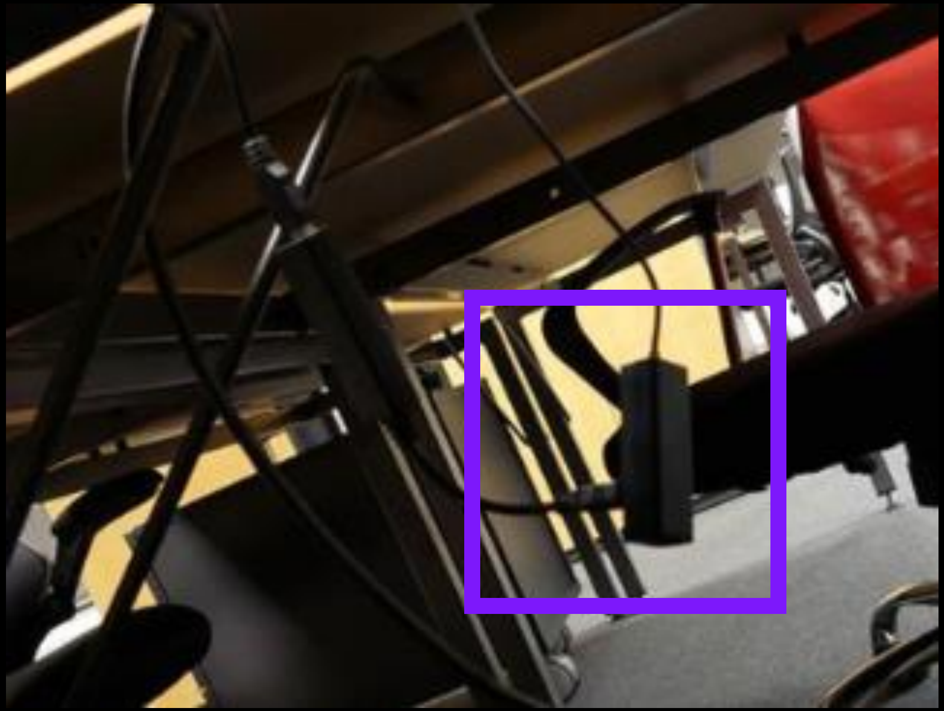
First of all good job on phishing exercise, I will share the results shortly. Meanwhile, I have modified some settings regarding vacations. They will go into effect from 2024. Please take a look at Microsoft Sharepoint[redacted]) - Vacation_list.xlsx. Feel free to ping me if you have any questions.

Example Case #3 – ? Device



Example Case #3 – Key Croc (Keylogger)

- Before Execution:
  - Enumeration on Internal resources
  - Exploring on-site
  - Testing with same model keyboard
- Execution
  - Planted after workday
  - Blue Team alerted victim as soon as the victim has typed his password and logged in.



Example Case #4 – Mail and phone

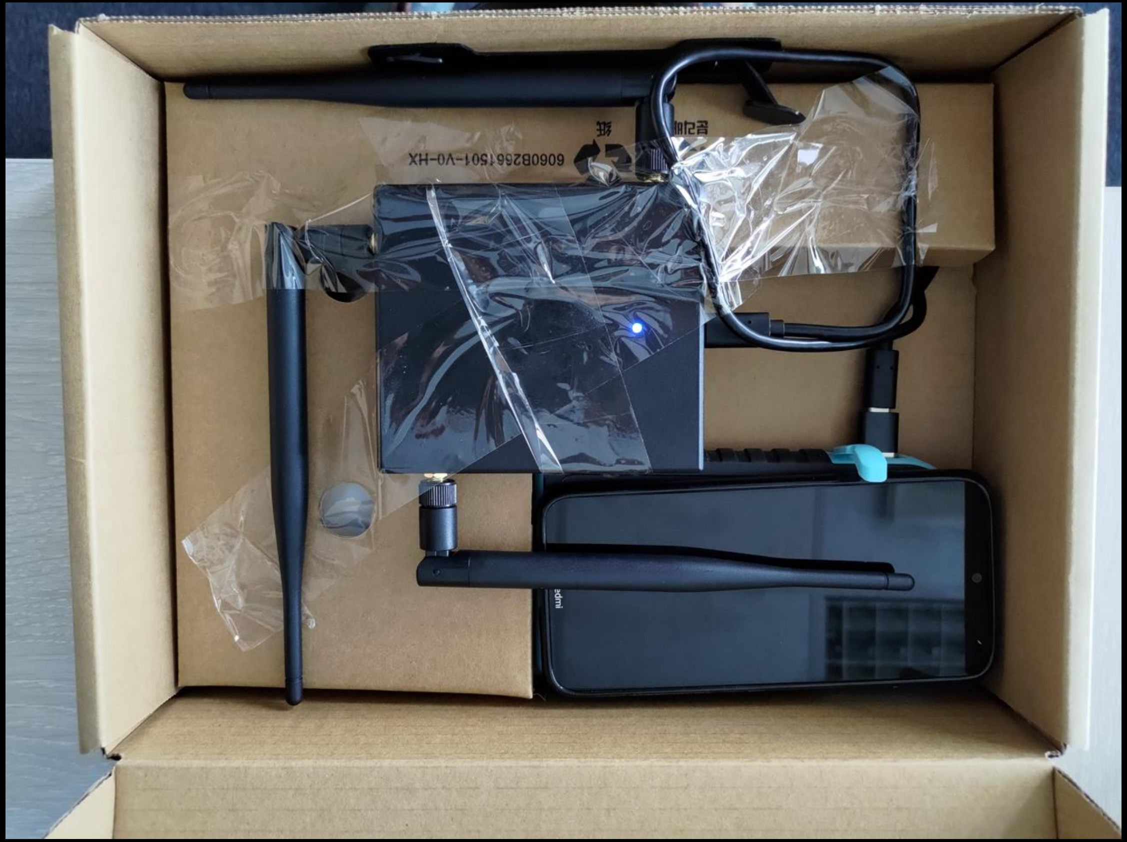
Security controls are too efficient?

- Before Execution:
  - OSINT
  - Landing page
- Execution
  - Got the creds ☺, but server info was missing
  - Phone phishing their service provider for missing information

Example Case #5 – WiFi

PineApple

- Before Execution:
  - Exploring on-site
- Execution
  - Planted behind ceiling
  - WiFi attacks



Improving Human Awareness

- **Continuous cybersecurity training**
    - Realistic simulations
- **Cybersecurity Awareness Training Programs**
    - Use quizzes, videos, and hands-on simulations to engage users
- **Security Policies and Best Practices**
    - Develop and communicate clear cybersecurity policies