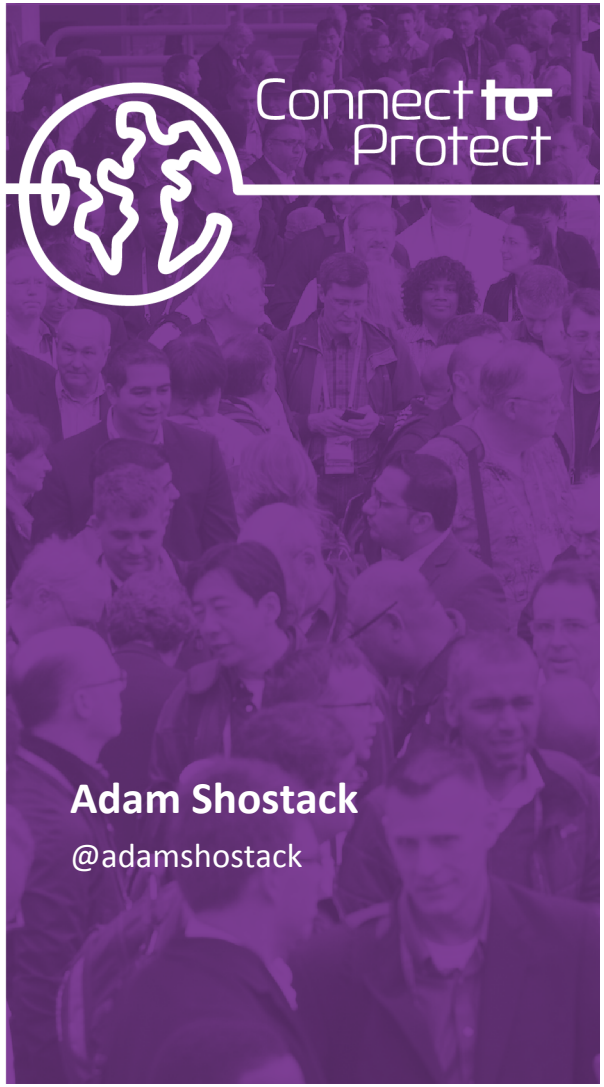
RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center



SESSION ID: HUM-R05

Securing the "Weakest Link"

Usable Security Lessons From Star Wars

Adam Shostack

@adamshostack

#RSAC

My real slide is too big to distribute

- In the room, there was video from “Star Wars” (fairly used!)
- It’s the boardroom briefing scene
- The general says “This battle station is now the ultimate power in the universe,”
- Vader responds “Don’t be so proud of this technological terror you’ve created”

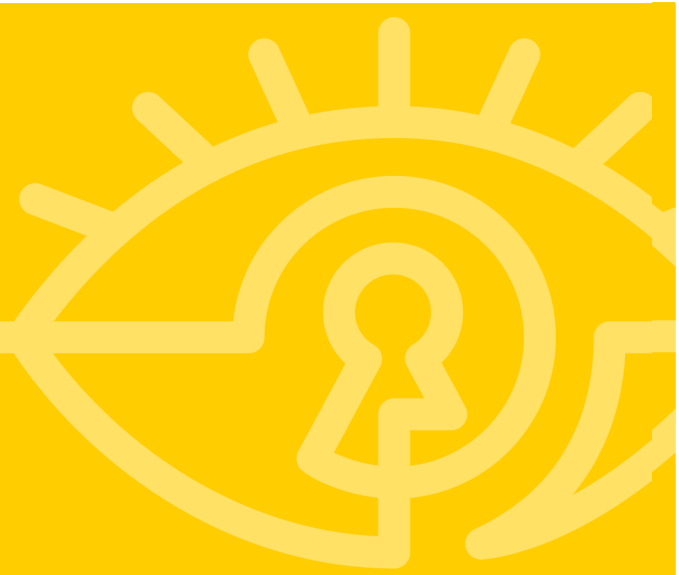
Lord Vader Was Right

USING THE FORCE

- Computer security is about people
- People are a motivated and struggling link
- We ignore the human element at our own risk

AGENDA

- Some threat models
  - How we make it worse
  - How people are exploited
- How to make it better



A Threat Model

A Bad Threat Model

"Given a choice between dancing pigs and security the user will pick dancing pigs every time"

An Even Worse Threat Model

- Declare the problem unsolvable!

OMG NOT OUR FAULT!

"IT security professionals can only do so much if an employee clicks on a spear phisher's link, creating a hole in your network."

Learned Helplessness!

Remote Desktops?

Web proxies?

People Get Tricked: A Threat Model

- Human action(s) to change the computer's configuration
  - Normal behaviors
  - No attacker says "now add a key to the registry" because FAIL
- The computer has a chance to intervene/mitigate
  - Warnings
  - Sandboxes
  - Architecture

How People Are Tricked

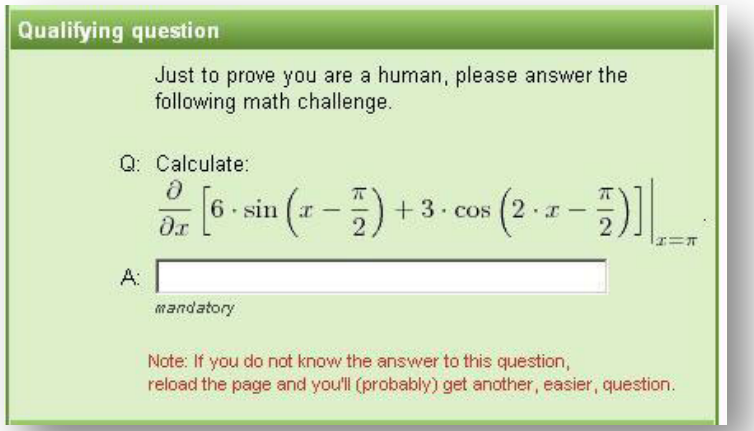
- Credential exposure (including phishing)
- Intentionally running or installing software
  - Codecs, doppelgangers and “Microsoft Support” calls
  - Pirated software with extras
- Accidental software execution
  - File extension hiding, icon tricks (Salaries.xlsx.exe)
  - Documents with exploit payload
- Web fakery — clickjacking, XSRF, etc

How People Are Tricked: Scamicry

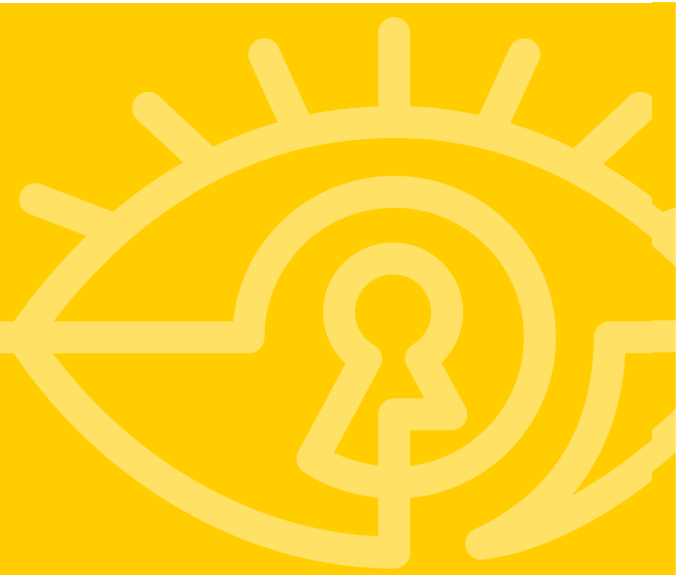
- Scamicry: When real messages imitate scams
- People have a security goal like “examine links carefully”
  - Store sends email with `<a href=“http://cts.vrecc.com/ls?39389ee28a/64f53b0c9c/http%3A%2F…>Safe Online Banking</a>`
  - Bank calls and asks for your password
- “But it’s the bank … I’m not smart enough to understand this”

How People Are Overwhelmed

- Advice that can't be followed in reasonable time
  - "Read TOS, privacy policies to understand how we'll use your data"
- Advice that requires too much skill
  - Solve this captcha!
- Complexity and depth
  - Why do you need a long password?
  - Let me explain password cracking…



http://www.seosmarty.com/impossible-captcha-it-doesnt-really-matter-if-you-are-human-or-not/



You Can Make It Better

Firefox Malware Warning

Reported Attack Page!

This web page at www.mozilla.org has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here! | Why was this page blocked?

Ignore this warning

Chrome Malware Warning

chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to malware.testing.google.test for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

Real World Click-through Rates

7.2% (Firefox Malware)

23.2% (Chrome Malware)

9.1% (Firefox Phishing)

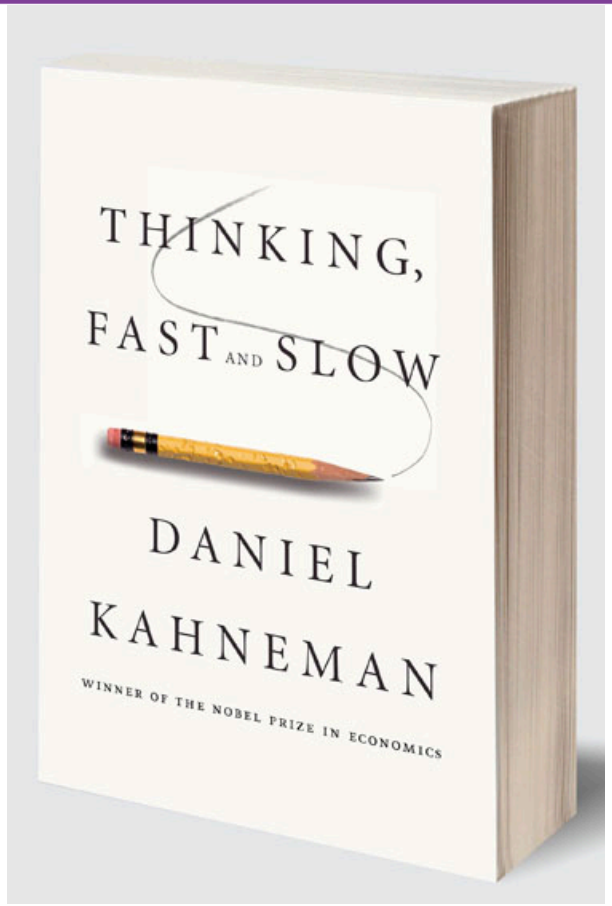
18.0% (Chrome)

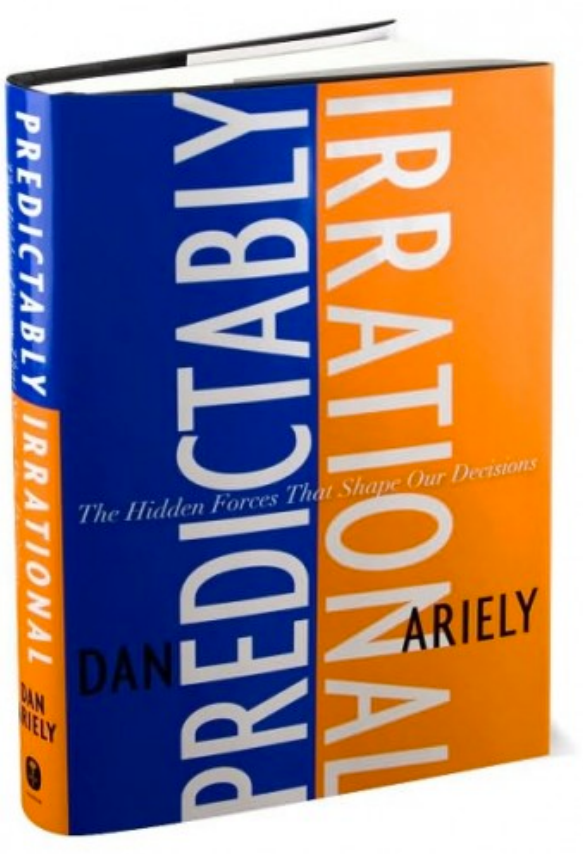
Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness

Threat Modeling & People

- A model of the system being developed (whiteboard, DFD)
- A model of the threats (STRIDE, attack tree)
- [New!] A model of the person using the software

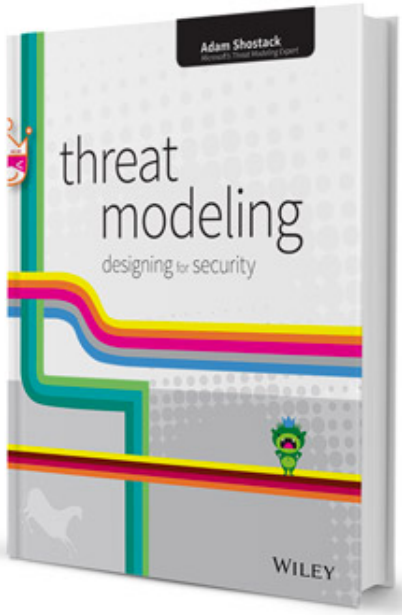
Threat Modeling and People





Threat Modeling and People (2/2)

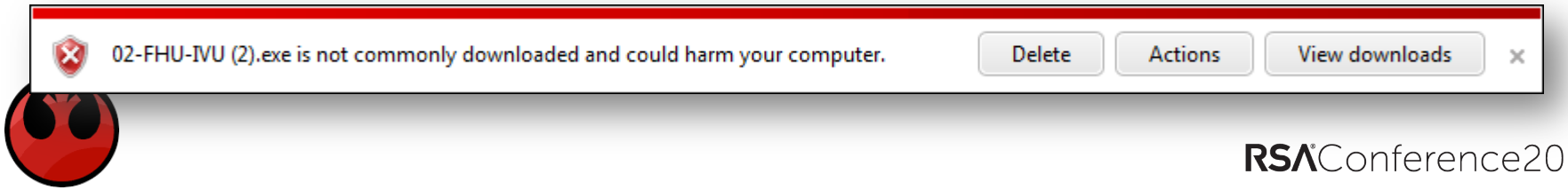
- A model of the person using the software
  - Behaviorist and cognitive science
  - Kahneman's System 1/System 2
  - Reason's "Strong Habit Intrusion"
- Models for usable security
  - Ellison: Ceremonies
  - Cranor: Human in the loop
  - Sasse: Compliance Budget



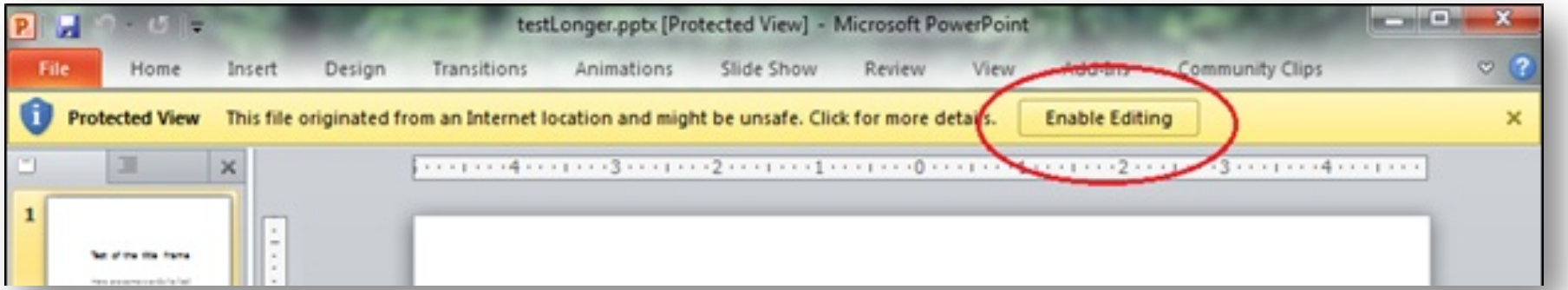
Threat Mitigations/Patterns That Work (Software developers)

Win by Building better defenses

- 2 Key patterns in Internet Explorer 8+
- Not warning on every download
  - People become habituated, click through
- Not making the dangerous choice the default



Patterns: Gold Bar



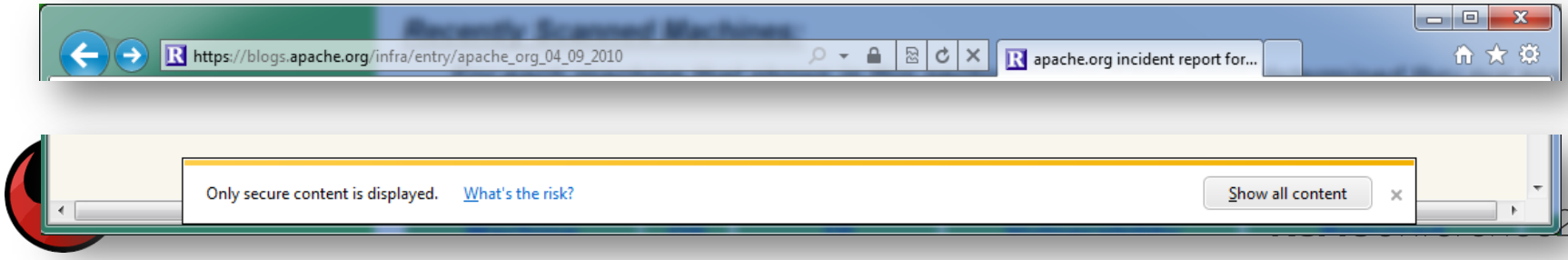
- Appears in Office, IE, Firefox, elsewhere

Engineer NEAT Warnings

- NEAT is an easy way to remember key security UX guidance
- NEAT
  - Necessary, Explained, Actionable, Tested
- Philosophy:
  - Don’t involve the person if you don’t have to
  - If you involve the person, enable them to make the right decision
  - Does the person have unique knowledge the system doesn’t?

NEAT Warnings: Necessary

- Avoid interrupting the user with security decisions, if possible
- When possible, automatically take the safest option and, optionally, notify the user that other options are available
- If people have no course of action & no unique knowledge, you should re-architect product



NEAT Warnings: Explained

- Provide the user with all the information necessary to make the right decision
- 6 key elements: SPRUCE
  - **Source**: Where is this decision coming from?
  - **Process**: What steps should they take to make the decision?
  - **Risk**: What is the security risk of getting the decision wrong?
  - **Unique Knowledge User Has**: What does the user know that we don't that helps make the right decision?
  - **Choices**: What are their options? What do we recommend they do? What will happen when they choose each option?
  - **Evidence**: What information should they factor in?

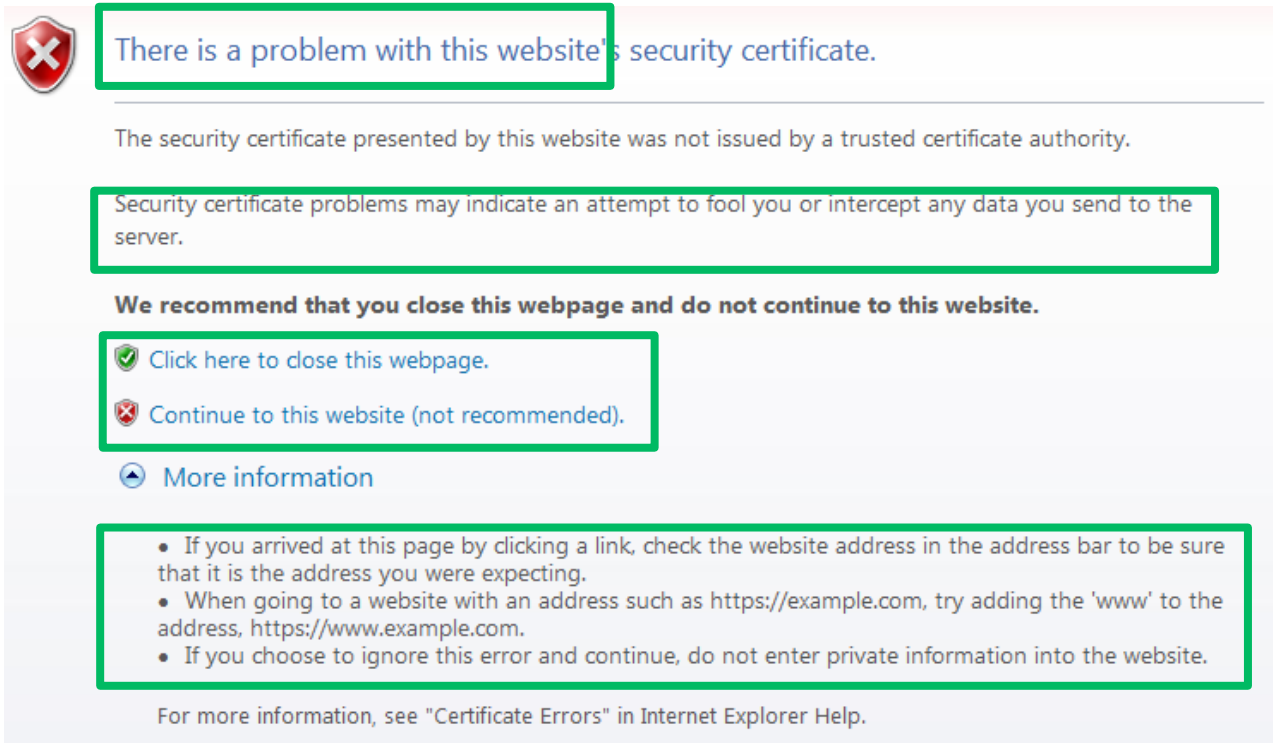
Good (long) example of explanation

Source

Risk

Choices

Process



Explanation: Opinionated Design

- Clear instruction
- Attractive preferred choice
- Unattractive alternate choice

From the Google Chrome team — “Improving SSL Warnings Comprehension and Adherence” by Adrienne Porter Felt & many colleagues

NEAT Warnings: Actionable

- Enumerate scenarios at design time
- Steps the person must take
  - Figure them out
  - Write them down
- Wording can be a tricky balance
  - Too wordy, people won't read or understand
  - Not enough information == not actionable

NEAT Warnings: Tested

- Validate your Security UI with real people
  - Benign and malicious scenarios
- Whole arsenal of UI testing techniques
  - Range from empaneling 1000s of people, to testing dozens in usability lab, to asking coworkers down the hall
- Apply what you can
- User tests are always surprising

NEAT Warnings: Wallet Cards

Microsoft

Ask yourself: Is your security or privacy UX:

NECESSARY? Can you change the architecture to eliminate or defer this user decision?

EXPLAINED? Does your UX present all the information the user needs to make this decision? **Have you followed SPRUCE? (see back)**

ACTIONABLE? Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

TESTED? Have you checked that your UX is NEAT for all scenarios, both benign and malicious?

NEAT

When you involve the user in a NEAT security or privacy decision, explain the decision using these 6 elements:

SOURCE: State who or what is asking the user to make a decision

PROCESS: Give the user actionable steps to follow to make a good decision

RISK: Explain what bad thing could happen if the user makes the wrong decision

UNIQUE KNOWLEDGE user has: Tell the user what information they bring to the decision

CHOICES: List available options and clearly recommend one

EVIDENCE: Highlight information the user should factor in or exclude in making the decision

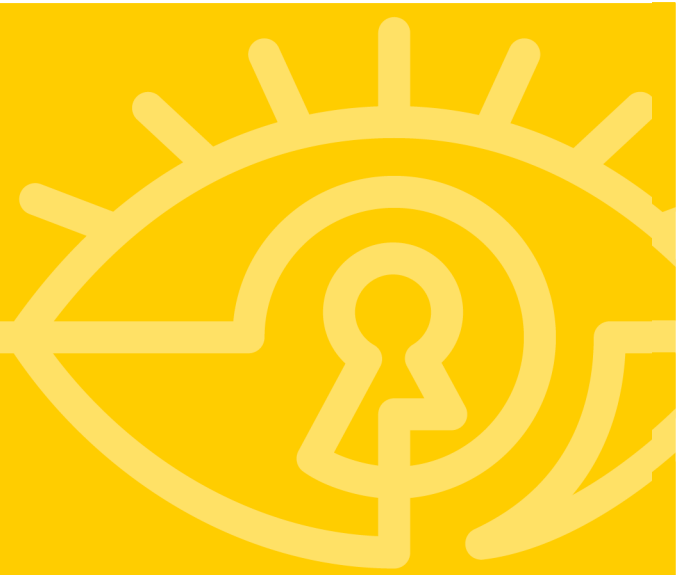
SPRUCE

For more info, contact **neatux@microsoft.com**

https://blogs.microsoft.com/cybertrust/2012/10/09/necessary-explained-actionable-and-tested-neat-cards/

RSAConference2016

#RSAC



Defensive Patterns That Work (Operations)

Spend Your "Budget" Wisely

- People want to get their job done
  - They expend effort to do it safely — to a point
- What do you want the most?
  - Are password changes worth the time?
  - Do you patch during the business day?
- Make it easy and fast to do what you want the most
  - Great opportunity to learn from marketing & UI experts

Example: Advice You Give

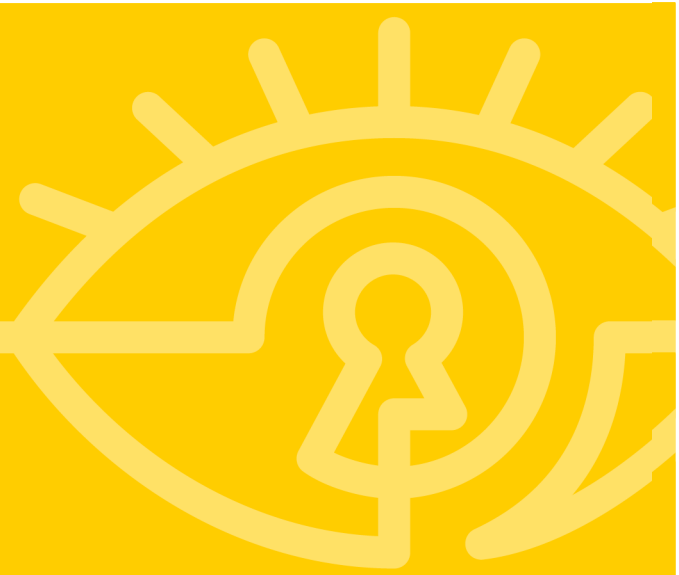
- Email is a threat vector
- How well do you help employees manage it?
  - Prevent: Is it easy to see who an email is legitimately from?
    - How often do your vendors email employees with demands?
  - Detect: How easy is it to report suspicious emails?
  - Respond: How quickly do you respond to those reports?
    - To the originator? To the recipient?
  - Are you breaking your own advice with scamicry?

Usability matters talking to executives

- Executives are skilled at managing risks
- We show up with the wrong messages
  - Compliance requirements
  - “Phone books” of risks
- “Cyber Defense Matrix” is a good step
  - Sounil Yu’s talk “Understanding the Security Vendor Landscape Using the Cyber Defense Matrix” (PDIL-W02F)

Apply Slide

- Don’t give in to the dark side
- Avoid confusing people with scamicry or impractical advice
- Use defensive software patterns
  - Gold Bar
  - Default Safe
  - NEAT
- Build operations for real people
- Share your work



Questions?
Thank you!