SOME MATERIAL BORROWED FROM MICHELLE MAZUREK, LORRIE CRANOR, MIKE REITER, ROB REDDER, BLASE UR, AND DAN VOTIPKA

1/14/26

USABLE SECURITY AND PRIVACY

CSCI 588: INTRODUCTION TO HUMAN FACTORS IN SECURITY AND PRIVACY

TODAY'S COURSE

- What is usable security and privacy?
- Why is usable security and privacy hard?
- How do we make security and privacy more usable?

WHAT DO YOU THINK IT MEANS FOR S&P TO BE USABLE?

THE HUMAN THREAT

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations… but they are sufficiently pervasive that we must design our protocols around their limitations."

—– C. Kaufman, R. Perlman, and M. Speciner. *Network Security: PRIVATE Communication in a PUBLIC World.* 2nd edition. Prentice Hall, page 237, 2002.

WHY SHOULD SECURE SYSTEMS CONSIDER USABILITY?

WHY SHOULD SECURE SYSTEMS CONSIDER USABILITY?

HOW CAN A LACK OF USABILITY LEAD TO BAD SECURITY/PRIVACY?

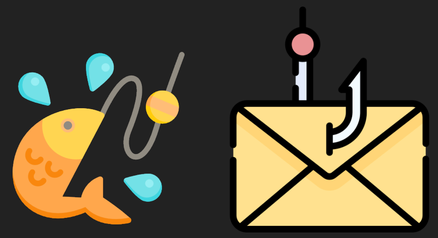
- Security vs productivity
- Humans take the path of least resistance
  - When security is hard, humans will circumvent it
- User error and fatigue - confusing/excessive warnings/interfaces lead to fatigue
- Leads to:
  - Failed adoption
  - Increased vulnerability
  - Lost productivity and cost

KEY CHALLENGES OF USABILITY

- Security terminology is complex and confusing
- Security is a secondary task
- Human capabilities are limited
- Misaligned priorities
- Habituation

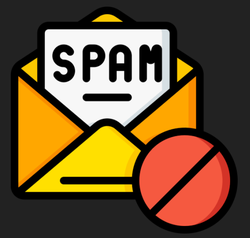
CHALLENGE #1: SECURITY TERMINOLOGY IS COMPLEX AND CONFUSING

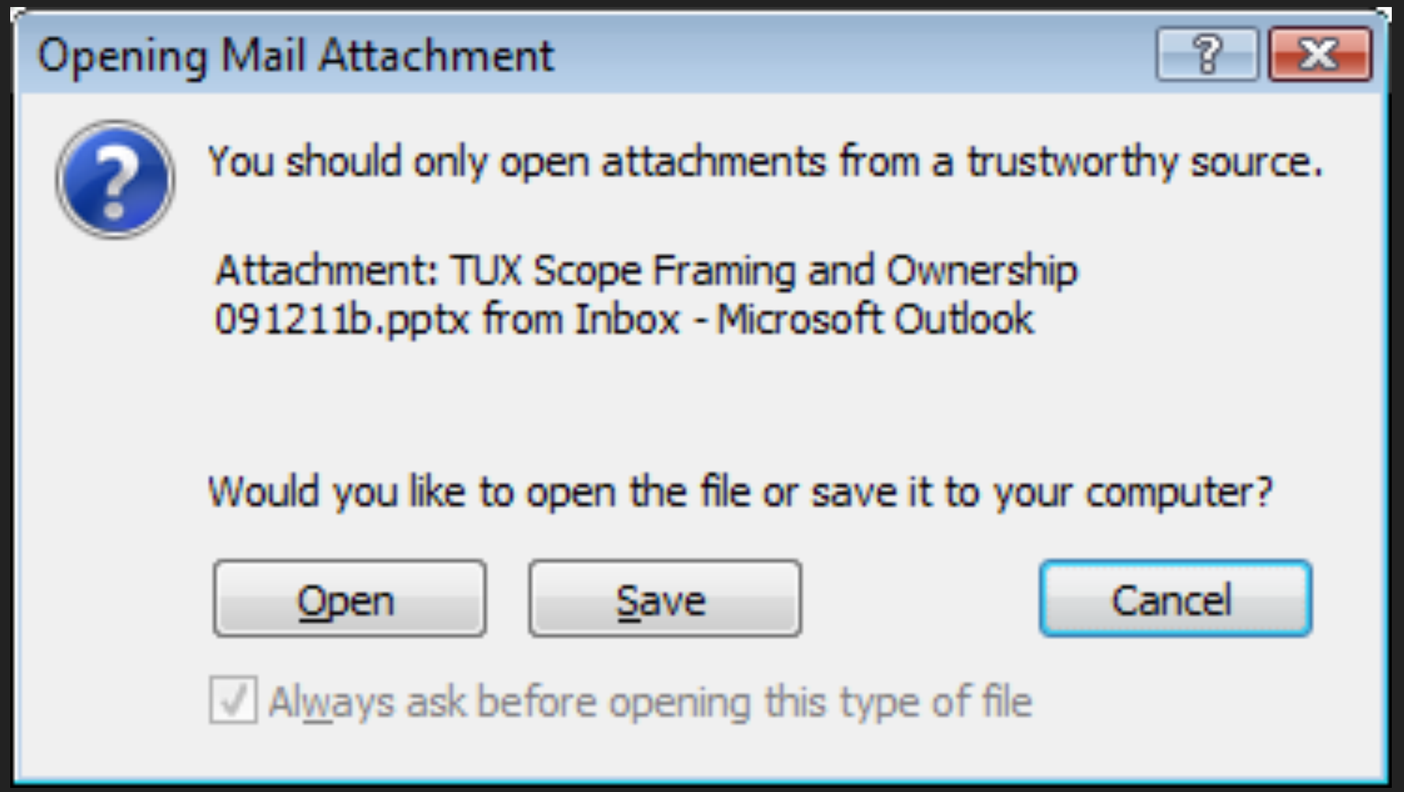
Phishing

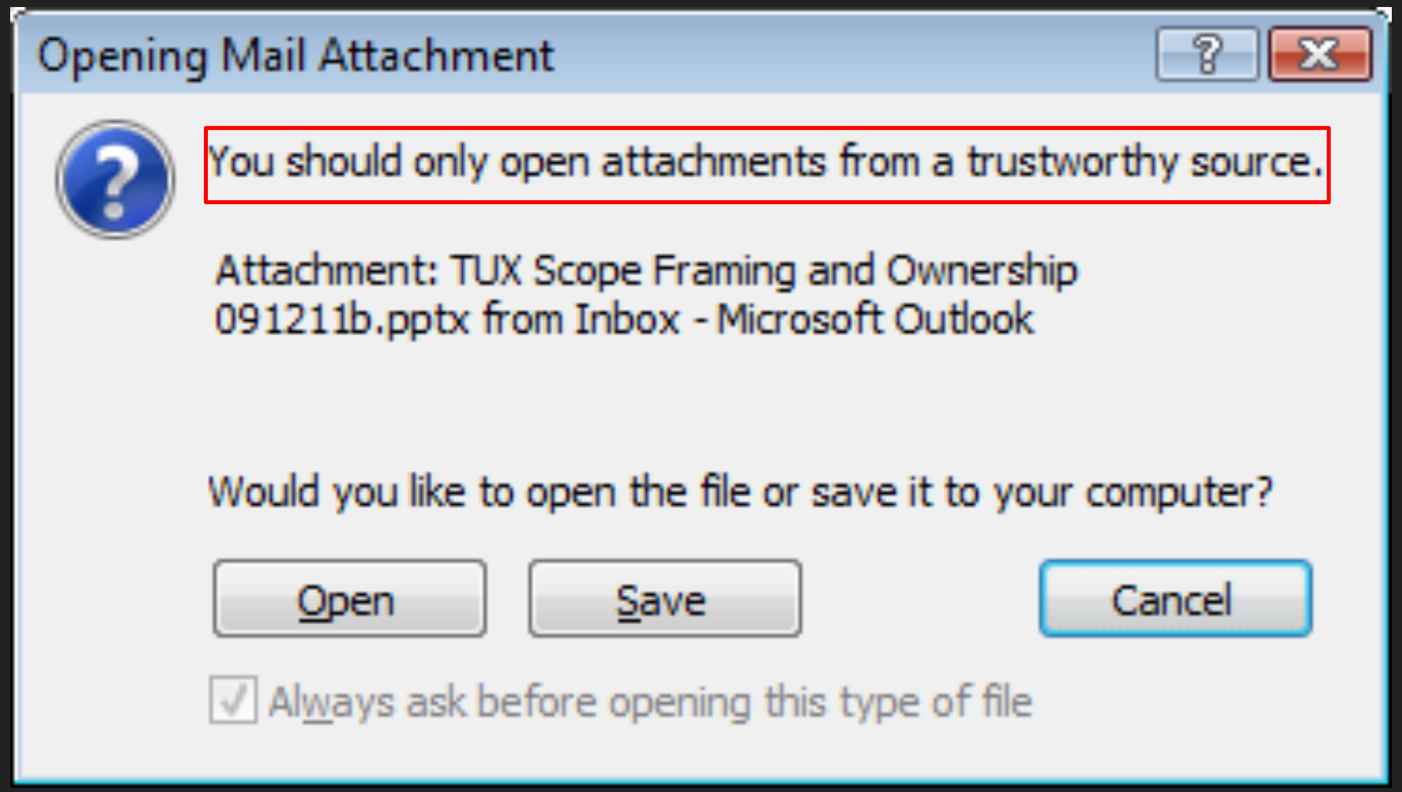


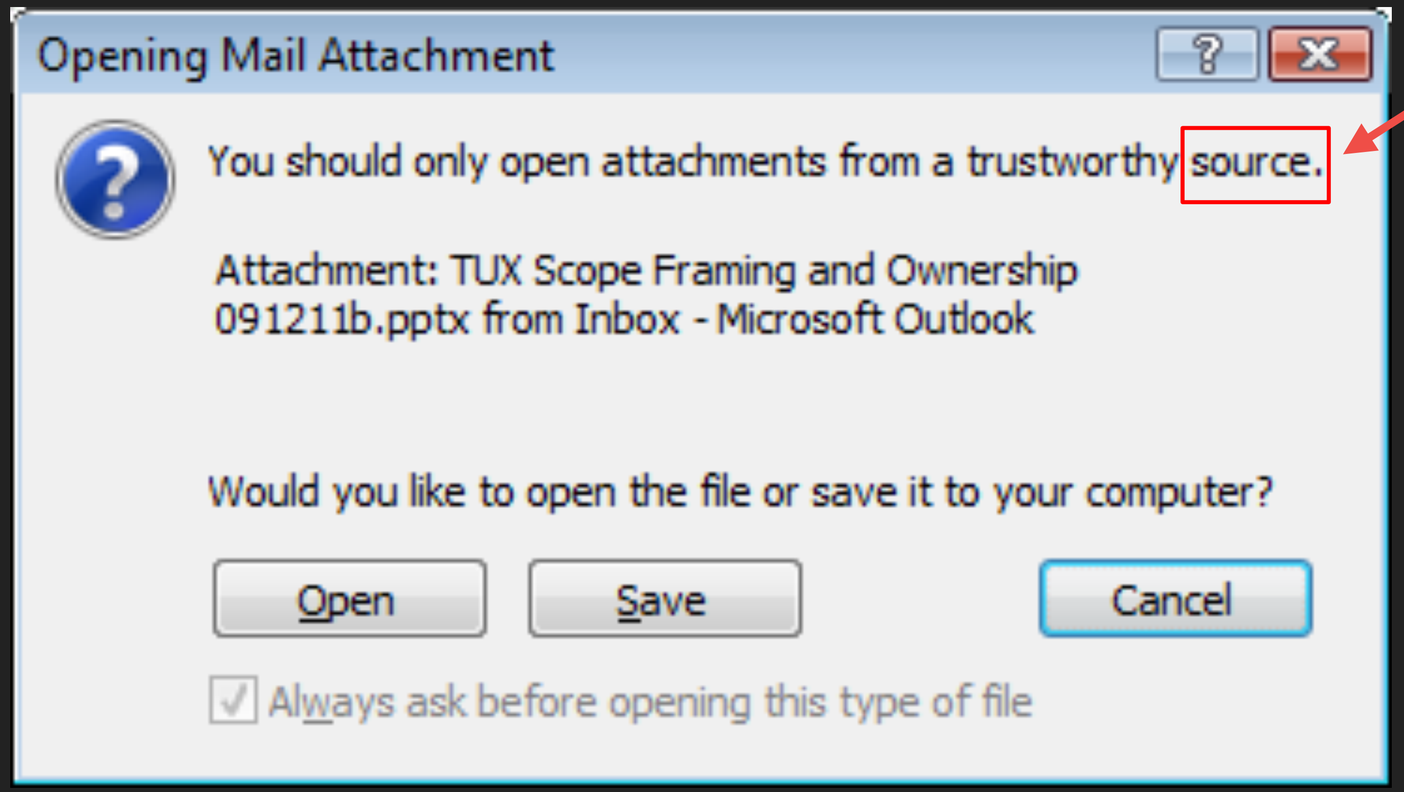
Virus

Spam

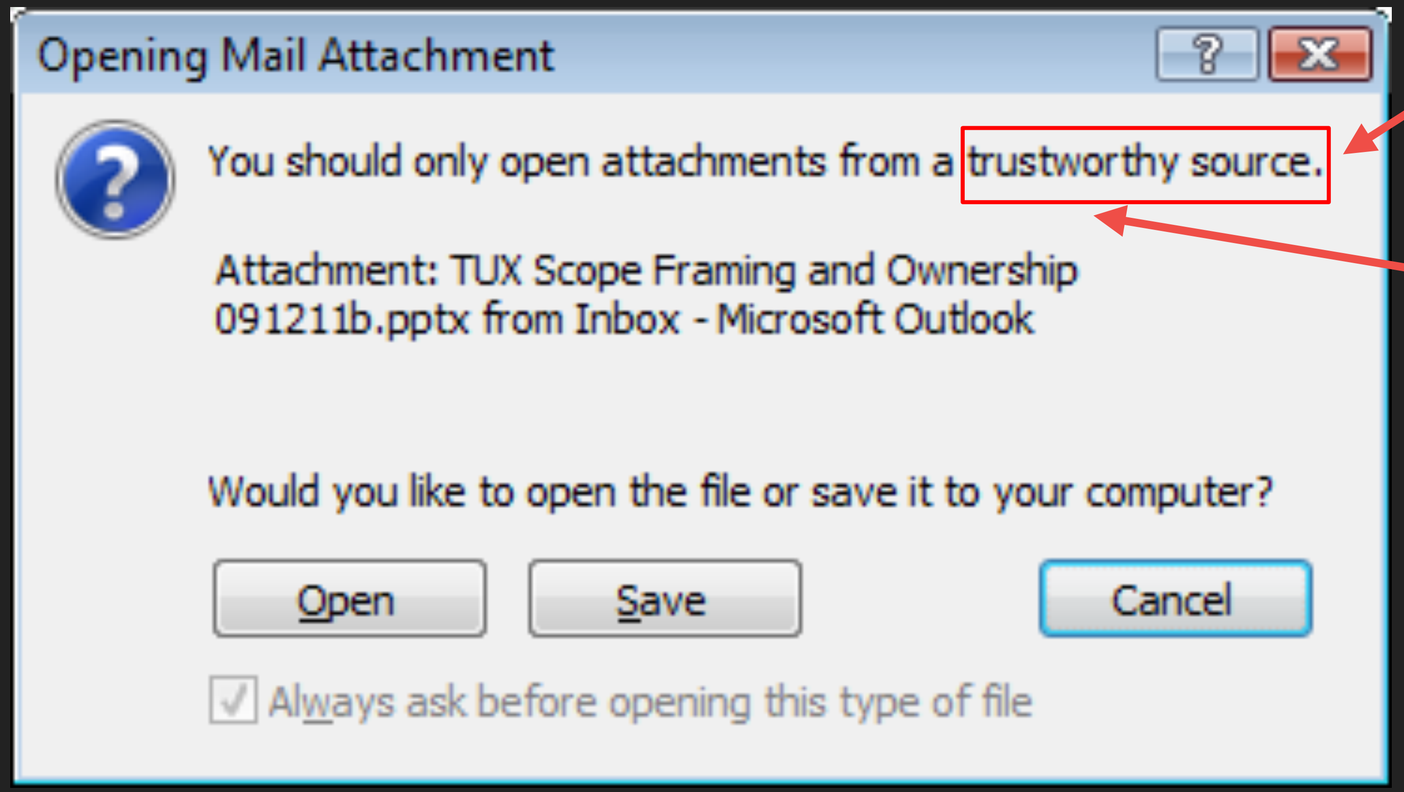



Opening Mail Attachment
You should only open attachments from a trustworthy source.
Attachment: TUX Scope Framing and Ownership
091211b.pptx from Inbox - Microsoft Outlook
Would you like to open the file or save it to your computer?
Open
Save
Cancel
Always ask before opening this type of file


Opening Mail Attachment
You should only open attachments from a trustworthy source.
Attachment: TUX Scope Framing and Ownership
091211b.pptx from Inbox - Microsoft Outlook
Would you like to open the file or save it to your computer?
Open
Save
Cancel
Always ask before opening this type of file



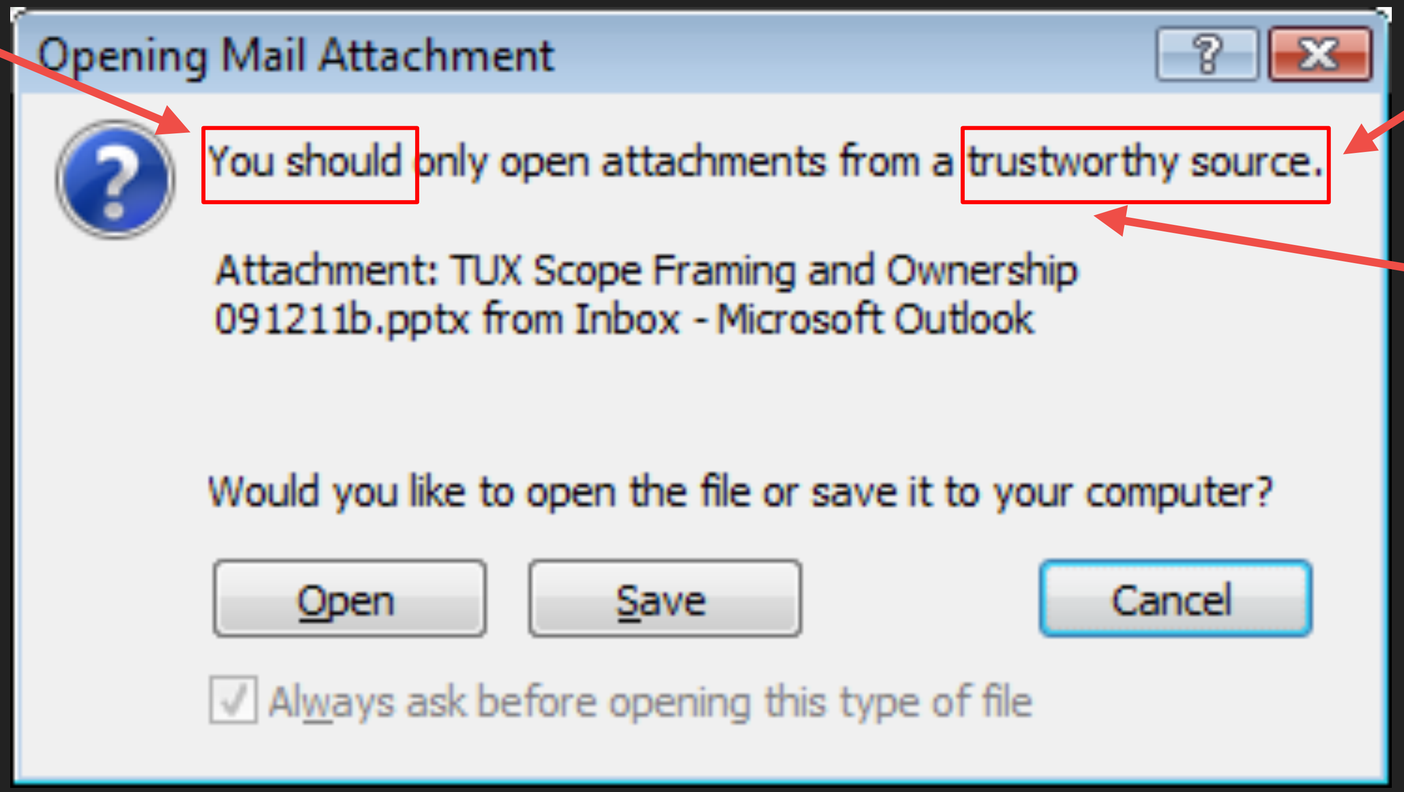
What is the source?



What is the source?

What makes a source trustworthy?

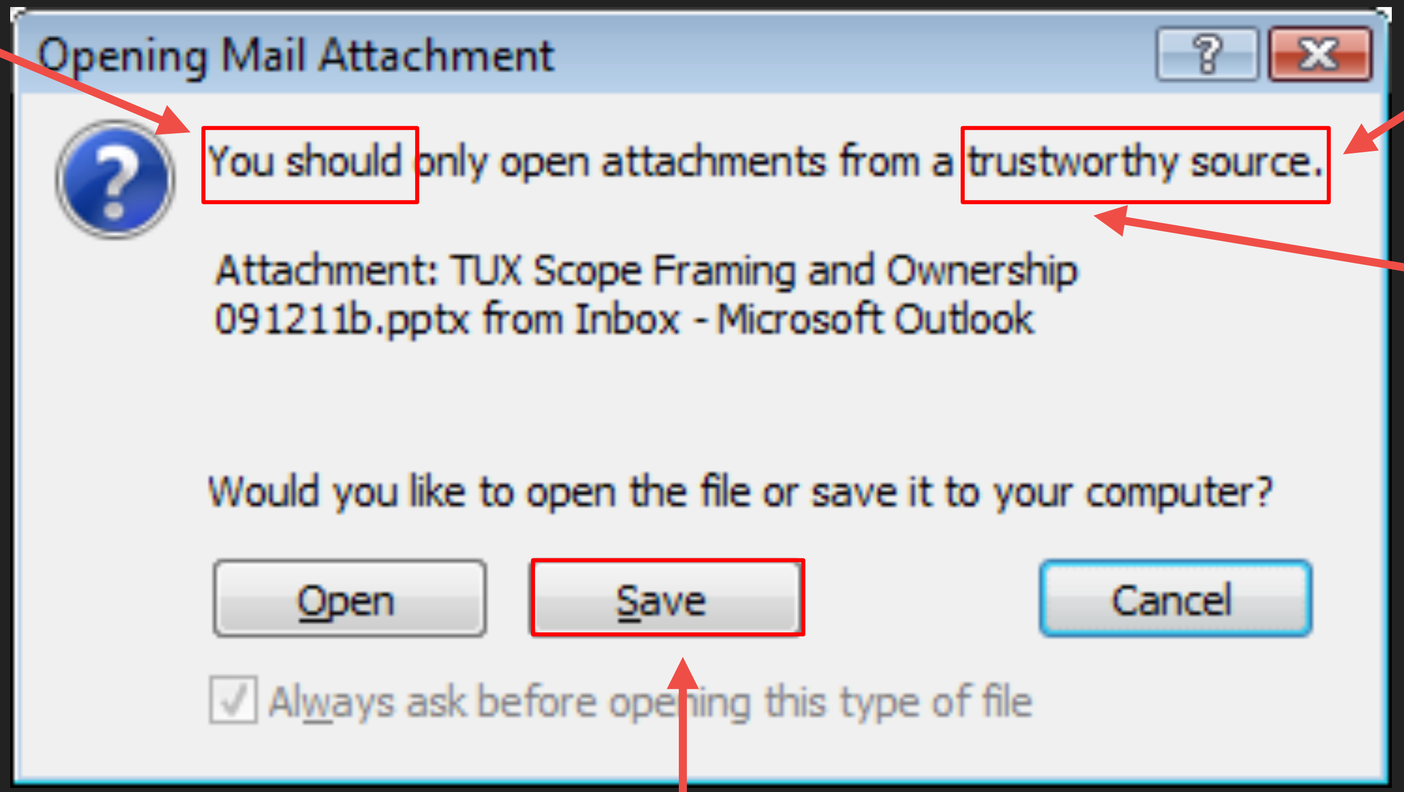
What happens if I don't?



What is the source?

What makes a source trustworthy?

What happens if I don't?



What is the source?

What makes a source trustworthy?

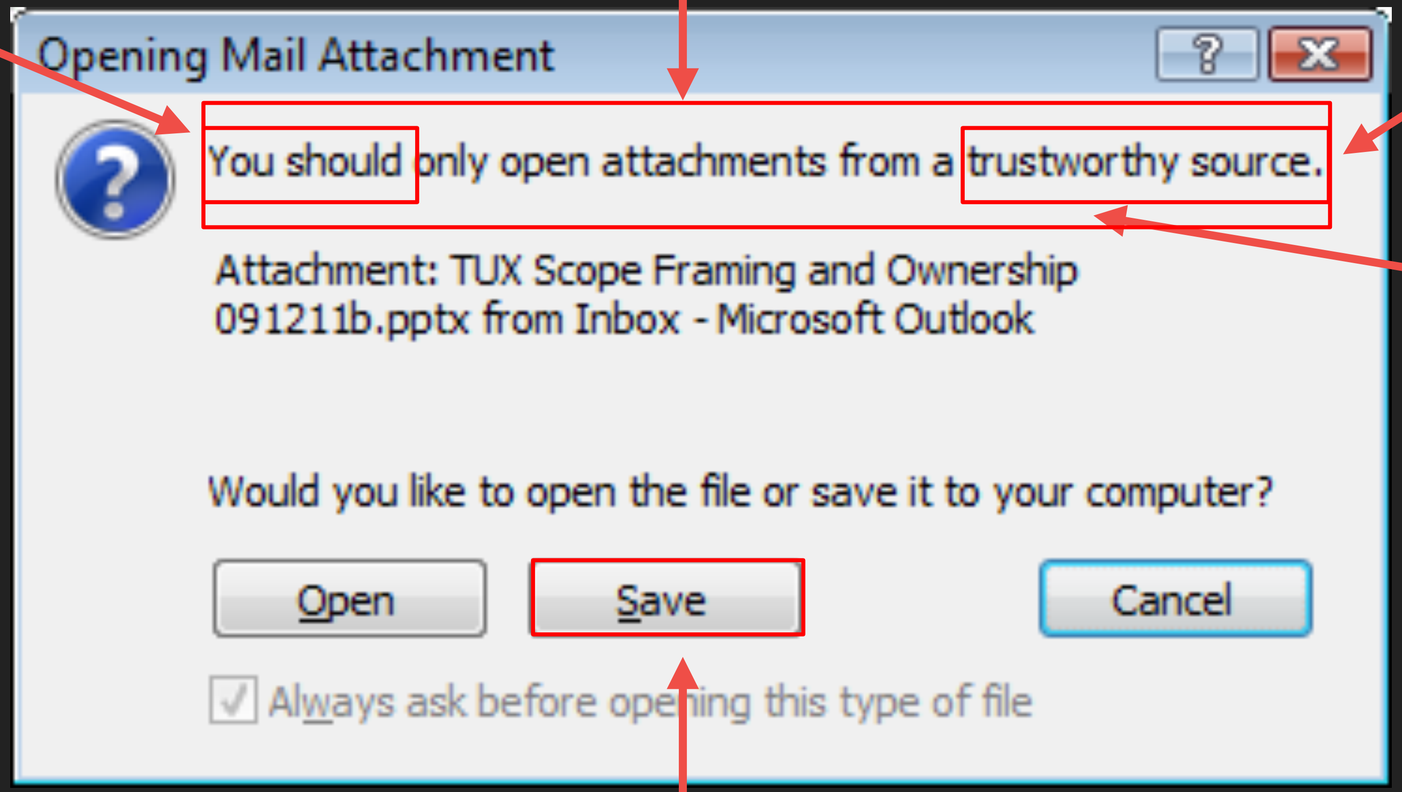
If opening is dangerous, is saving okay?

What happens if I don't?

How do I evaluate what to do?

What is the source?

What makes a source trustworthy?



If opening is dangerous, is saving okay?

WHY TERMINOLOGY MATTERS?

- People click “proceed anyway” but don’t understand risk
- Consent is rarely informed
- Poorly configured devices and data

CHALLENGE #2: SECURITY IS A SECONDARY TASK

- Given two paths to a goal, people will always take the shorter one
- More steps means something is less likely to be completed
- Hard to complete means something is less likely to be completed

RECOMMENDED SECURITY PRACTICES

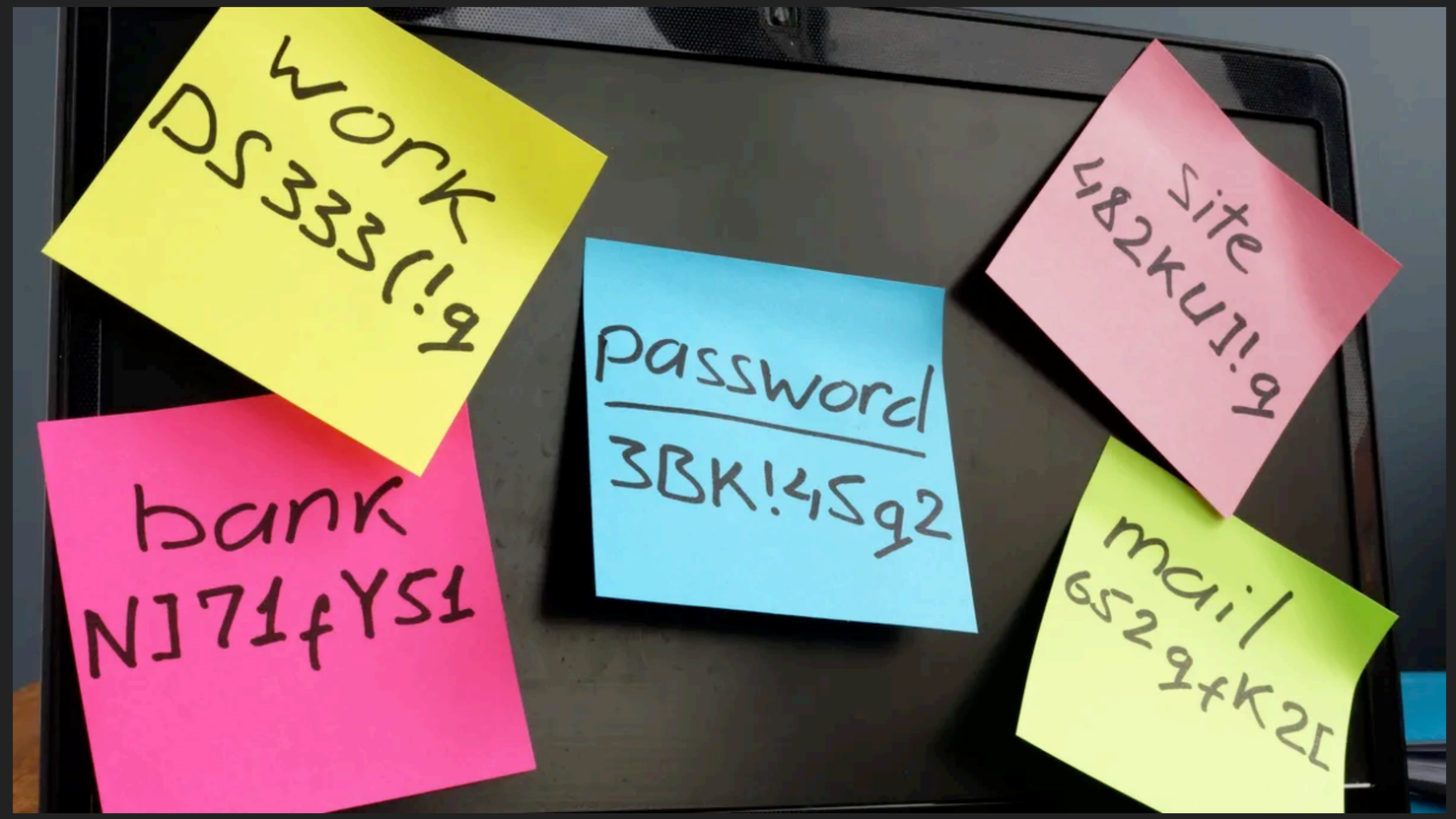
- Install anti-virus
- Keep apps and software updated
- Make strong, unique passwords
- Read websites' privacy policies before using
- Make regular back-ups of data
- Research software/apps before installing
- Regularly check accounts for unusual activity

WHAT HAPPENS WHEN SECURITY IS SECONDARY?

- People bypass or disable protections to complete tasks
- Security is a “speed bump”
- Systems are secure in theory, but not in practice

CHALLENGE #3: HUMAN CAPABILITIES ARE LIMITED

- Humans have limited memory, attention, and perceptual accuracy
- Can you remember a unique, strong password for every site?



LIMITED CAPABILITIES MEANS LIMITED SECURITY

- What do people do when they can’t remember unique passwords?
  - They write them down
  - They reuse them
  - They slightly change them
- People have increased vulnerability to attacks
- People have increased errors in judgment
- People rely on insecure shortcuts

CHALLENGE #4: MISALIGNED PRIORITIES

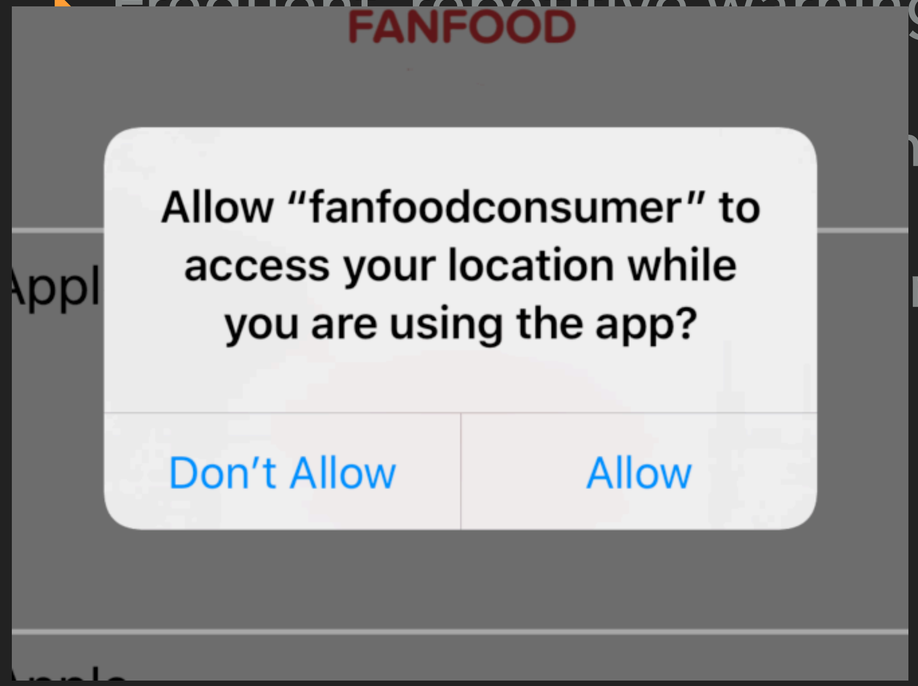
- Organizations optimize for security
  - Frequent password expiration
  - Overly strict access control
- People optimize for convenience and productivity
  - People write passwords down or make weak passwords
  - People use personal accounts or find workarounds

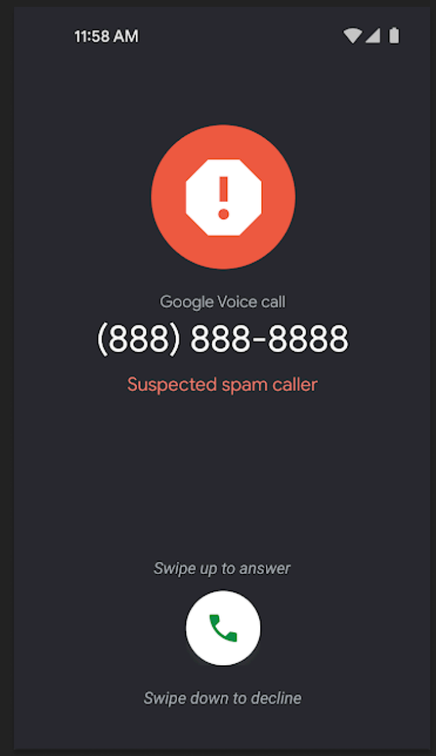
MISALIGNED PRIORITIES MEAN POORLY ADOPTED SECURITY

- People circumvent policies
- People are frustrated and don’t comply
- Push for security means that organizational security is actually weakened

CHALLENGE #5: HABITUATION

- We experience a lot of pop-ups and warnings in a day
- Frequent, repetitive warnings become less effective over time





BECOMING HABITUATED MAKES SECURITY LESS EFFECTIVE

- Overlook critical alerts because they weren’t an issue before
- Perceptions of risk become misaligned with reality
- Warnings are something that happen in the background

KEY CHALLENGES OF USABILITY

- Security terminology is complex and confusing
- Security is a secondary task
- Human capabilities are limited
- Misaligned priorities
- Habituation

DESIGNING FOR USABILITY

- Make security invisible
- Better interfaces
- User education

STRATEGY #1: MAKE SECURITY INVISIBLE

- Security works best when people don’t have to think about it
- Improve security by removing friction, reducing interruptions, and automating protection
- Helps address:
  - Security as a secondary task
  - Human limitations
  - Misaligned priorities

EXAMPLES OF INVISIBLE SECURITY

- Automatic updates (no prompts, no user decisions)
- Default-on encryption (users/developers don’t configure it)
- Alternate authentication (something you have or are)
- Invisible security measures should:
  - Reduce user burden
  - Eliminate opportunities for error
  - Ensure best path = easiest path

WHEN SHOULD SECURITY BE VISIBLE?

- High-risk actions
- Unusual behavior
- Decisions with serious consequences

STRATEGY #2: DESIGN BETTER INTERFACES

- Clear and intuitive interfaces help people make good choices
- Focus on clarity and transparency
  - Use plain language, Explain risks in easy terms
- Incorporate consistency and predictability
  - Reuse patterns, icons, and colors
- Provide actionable warnings
  - Tell users what to do along with the problem
  - Make safe choice clear

DESIGNING FOR HUMAN LIMITATIONS

- Make interfaces compatible with human behavior
  - Don’t design for the ideal, design for the real
- Reduce the need for memory
- Reinforce recognition over recall
- Keep decisions simple

STRATEGY #3: USER EDUCATION

- Design can only do so much. People need to understand S&P
  - Usually only at a high-level
- Education should be contextual, practical, and relevant

HOW DO WE EFFECTIVELY EDUCATE USERS?

- Just-in-time education
  - Provide short explanations at the moment an action is performed
- Scenario-based learning
  - Teach pattern recognition over strict rules
  - Provide real examples
- Hands-on training
  - Simulate real-world events

PRINCIPLES OF GOOD SECURITY EDUCATION

- Keep it short
  - Avoid long policy documents
- Make it relevant
  - Real risks tied to users' tasks
- Focus on behaviors
  - Rather than memorizing facts
- Reward positive actions
  - To reinforce good habits

A SYSTEM IS ONLY AS SECURE AS ITS USERS

- Usability is fundamental, not optional
- Security fails when users aren’t considered
- People are an important part of the system
- Secure systems don’t need users to be experts
  - But they do need to consider users