463.1 Introduction

Computer Security II
CS463/ECE424
University of Illinois

Two broad areas of past, current, and emerging interest

1.1. End-point Security (Today)

1.2. Critical Infrastructure Protection (Next Lecture)

463.1.1
End-point Security

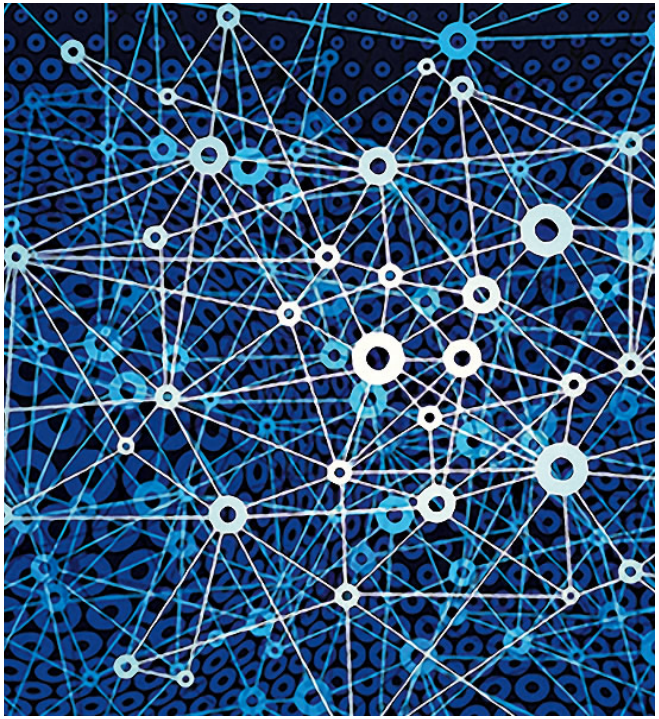
History

- Classical security work focused on multi-user, military and commercial systems
  - Not applied to desktop computers
- Early designs of desktop OS systems (which we are calling “hosts” for this discussion) included no security
  - Single user
  - Single address space
  - No permissions

Early Threats

- Viruses
  - Boot sector viruses (trading floppies)
  - Executable viruses (trading software)
- Defenses
  - Anti-virus software (e.g., Symantec)
  - Software hygiene - beware of shareware
- Mostly contained the problem

Big Change 1: Internet



- Constant data exchange
- Active attacks are possible
- Spread a virus/worm much faster
  - Email virus spreads in days / hours
  - Active worm can spread in minutes / seconds
- Anti-virus software not enough

Big Change 2: Complexity

- Software and data files become more complex
- Boundary between data & executable blurred
  - JavaScript, Java, Active/X
  - Word macros, PDF, …
- Data hygiene not as easy

Big Change 3: Motivation

- Attacks on hosts used to have little value
  - A virus got you fame, glory (& perhaps prosecution)
  - Serious attackers looked at commercial or military systems
- New motivations → new threat model
  - Financial gain: get access to bank accounts, credit card info
  - Disruption: disable critical infrastructure (e.g., WannaCry)
  - Politically motivated: publish stolen secrets on WikiLeaks

Other Challenges: Zero-day Exploits

- Malware that exploits previously unknown vulnerabilities
  - Potentially disastrous results
- Identify unknown malware
  - Scanning detection
  - Honeypots
- Address with automated signature generation
- Recovery strategies essential

Other Challenges: Human Factors

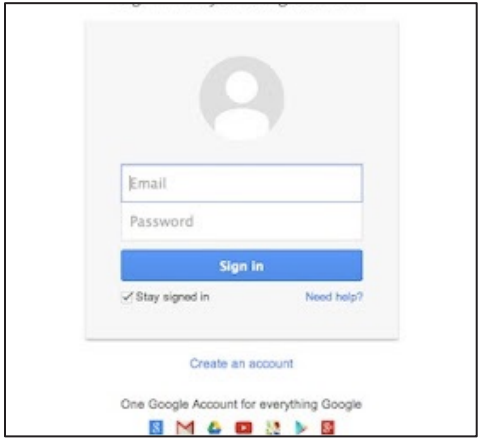
- Users specify security policy
  - Difference between a secure and insecure action is user intent
- Users can only make good decisions about something they understand
- Research in security turning to HCI: Humans are the last (and often weakest) link

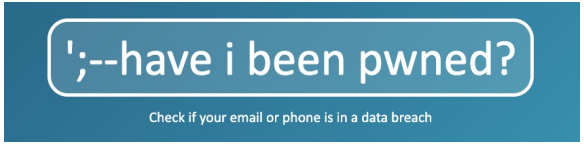
Case Study: User Authentication at End-Point

Why is “password” often insufficient to secure your account?

Data breaches expose user passwords

- Users often reuse passwords!
- A study (based on 62 million leaked passwords from 29 million users) shows:
  - 38% users have once reused the same password in two different services
  - 21% users once slightly modified an existing password to sign up for a new service [1]



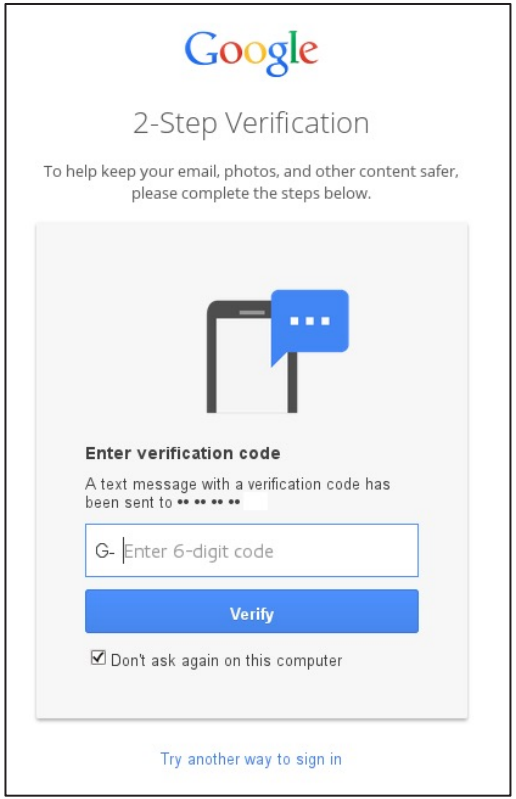


[1] The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services, CODASPY, 2018. https://gangw.cs.illinois.edu/pass.pdf

Case Study: User Authentication at End-Point

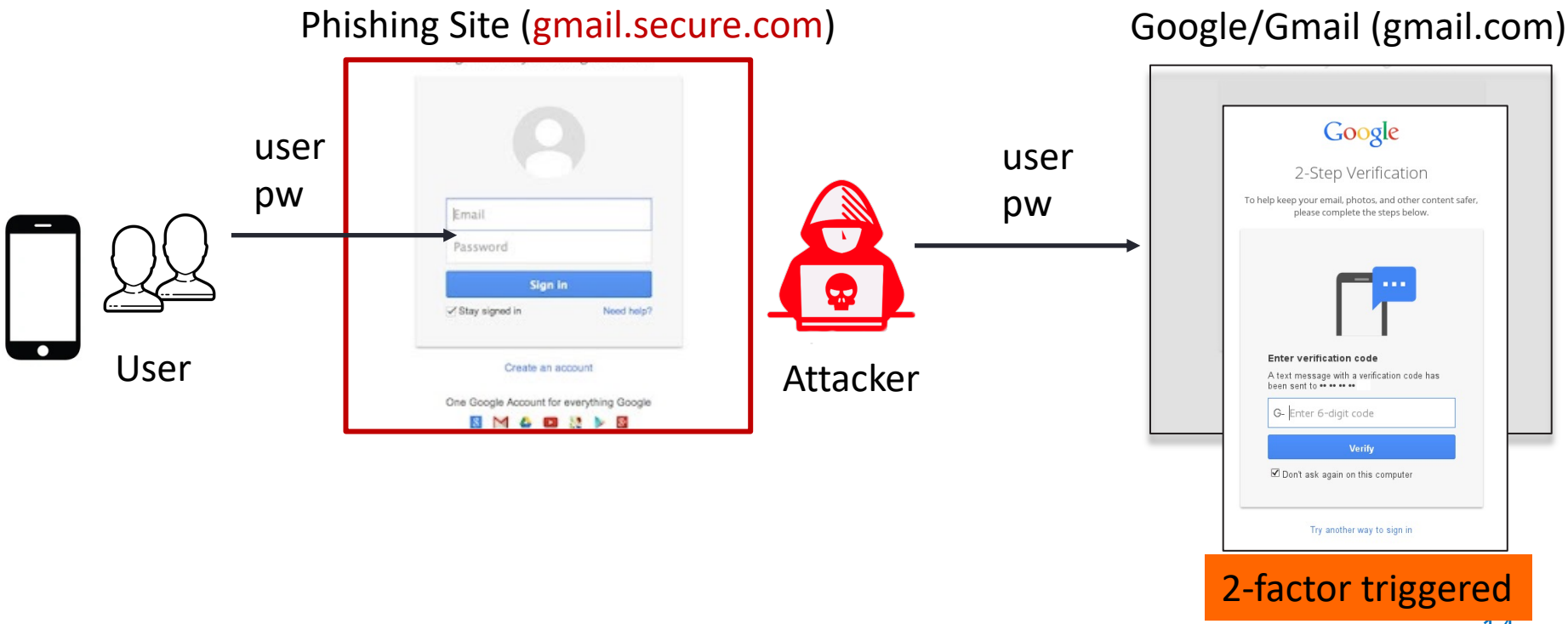
- How about two-factor authentication (2FA)?
  - Idea: an additional factor to verify who you are
  - SMS, DuoMobile, etc.

- Is 2FA secure enough?

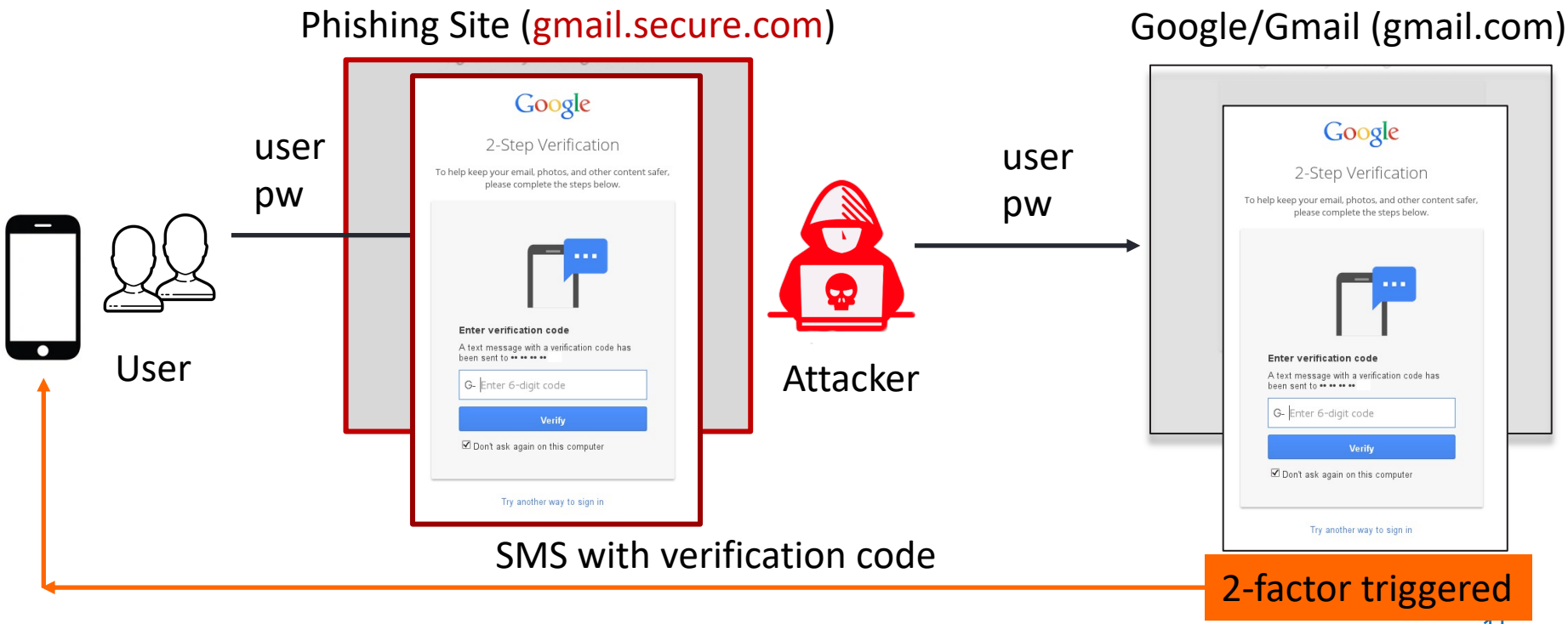


Bypassing Standard 2FA via Real-Time Phishing

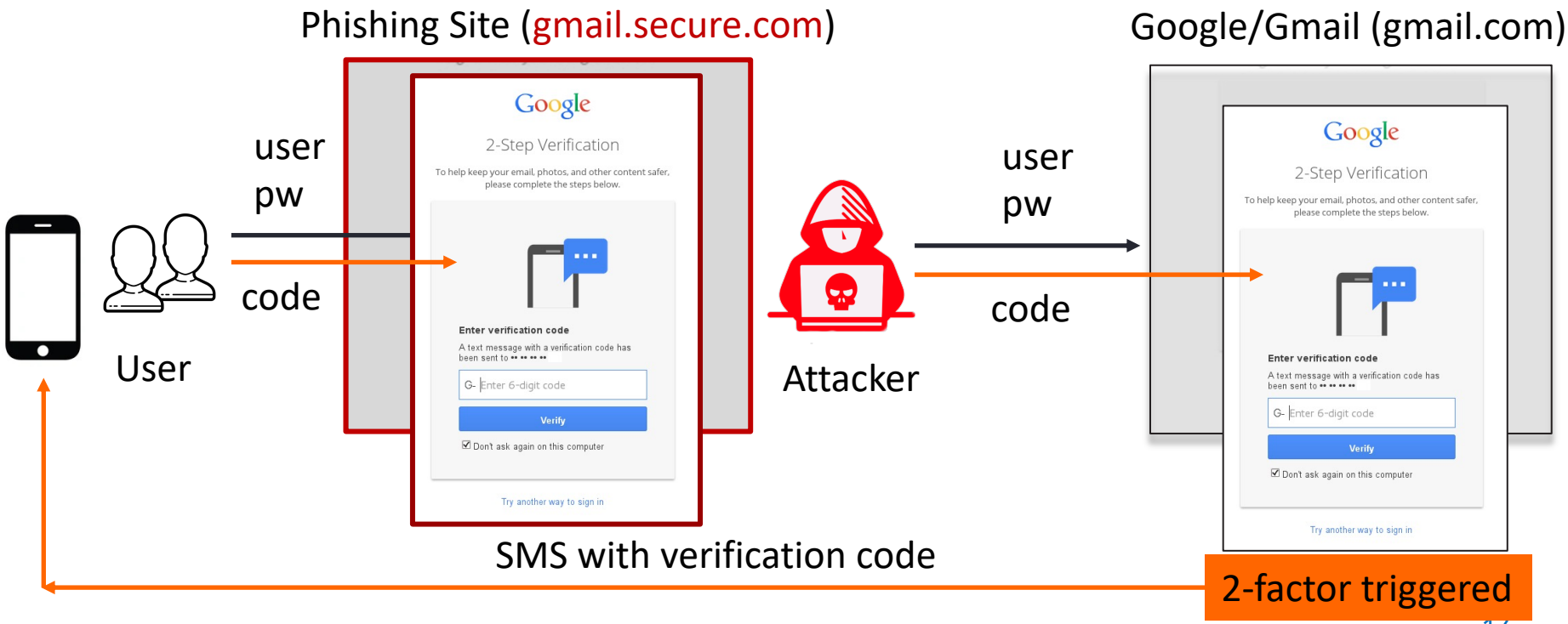
Bypassing Standard 2FA via Real-Time Phishing



Bypassing Standard 2FA via Real-Time Phishing



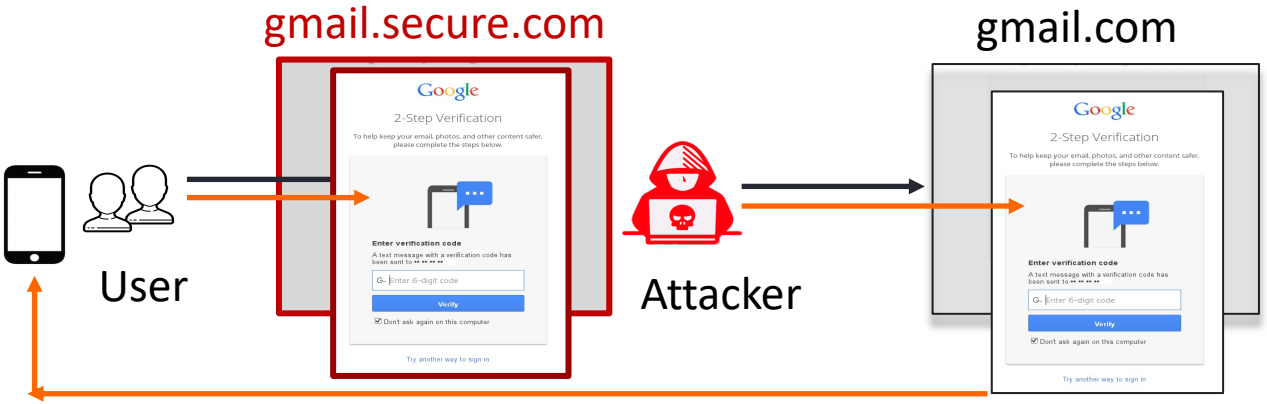
Bypassing Standard 2FA via Real-Time Phishing



Bypassing Standard 2FA via Real-Time Phishing

- Root cause: the phone (identity provider) cannot distinguish who sent the authentication request (real gmail vs. phishing), code not binded to website

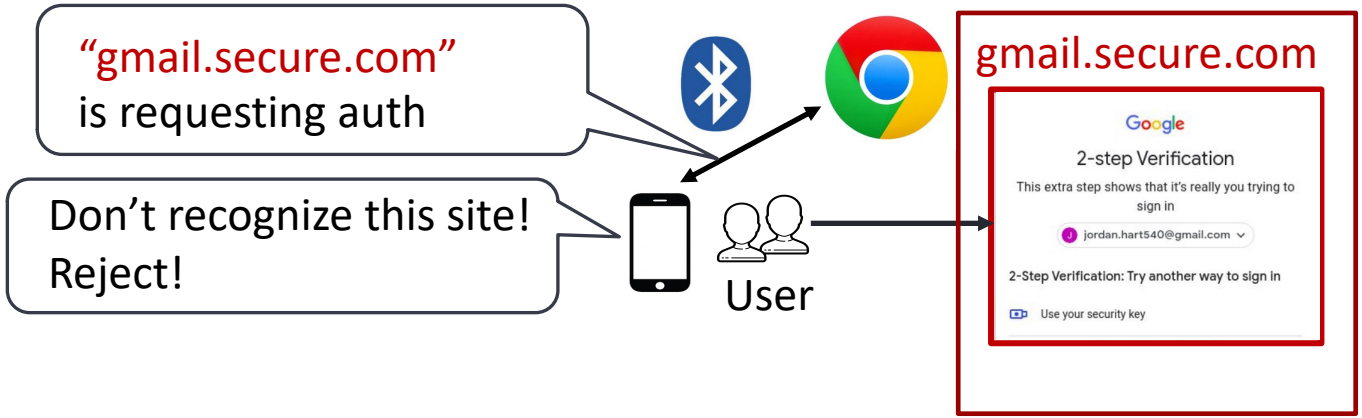
- One potential solution: FIDO Universal Second Factor (U2F)
  - The user's browser tells the authentication device (phone) which website is requesting;
  - A security token is unique for each website to avoid identity confusion



Bypassing Standard 2FA via Real-Time Phishing

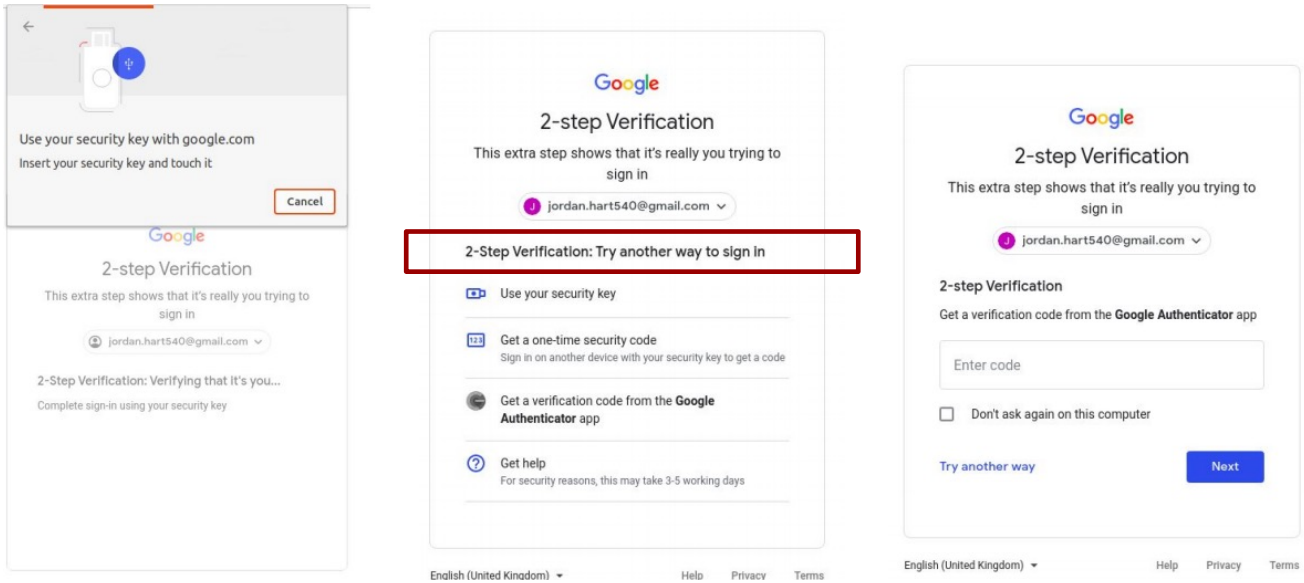
- Root cause: the phone (identity provider) cannot distinguish who sent the authentication request (real gmail vs. phishing), code not binded to website

- One potential solution: FIDO Universal Second Factor (U2F)
  - The user's browser tells the authentication device (phone) which website is requesting;
  - A security token is unique for each website to avoid identity confusion



FIDO Universal Second Factor is still not Perfect

- Downgrade attack against FIDO
  - Trick users to use less secure 2FA



Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols", USENIX Security, 2021.

References

- [1] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. “The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services”. In Proceedings of The ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018

- [2] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. “Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols”, In Proceedings of USENIX Security, 2021.