Usable Security and User Training

KAMI VANIEA

JANUARY 25

Think about it:
Is the Doodle link to the right secure?

KAMI VANIEA

1

First, the news ...


Users are not the enemy

- Malicious actors are the enemy
- Users are a partner in keeping the system secure
- Like any partner:
  - They have skills you don’t have
  - They are missing skills you do have
- Think about what skills they have that you need
- Use the skills you have to make good decisions on users’ behalf

Human in the Loop Framework
Phishing attacks and training

Phishing

- Phishing – Attempting to trick someone into taking the “bait” and interacting in a way they should not.
  - Typically involves the impersonator pretending to be someone else that the person trusts
  - Interactions: Clicking a link, opening a file, replying with information, transferring money, etc.
- Spear phishing – Phishing, but with a small number of targets and each email is crafted for that individual
- Whaling – Phishing for people with a lot of money, i.e. CEO
- QRishing – Phishing attacks through QR codes

What on this email can be trusted?

- Authority figure that often sends emails
- Clear threat to recipient’s ability to log in
- Trust indicators (Wrong)
  - False statement saying the email has been scanned and is safe

Problem: Users click on links and attachments

- Scan all incoming attachments and links for blacklisted content
- Teach users
  - Only click if you are expecting the email
  - Do not open attachments unless you are expecting them
  - If you are not sure, contact the person or company separately and ask if they sent the email
  - If you are not sure, contact the IT department
  - Banks and credit card companies will never contact you this way

Sneaky email to get the recipient to open the attachment, which is an html document

(Wrong) Trust indicators
Anti-Phishing Phill

Serious game to help people learn to spot dangerous URLs

Training sometimes works

But it takes time

And people forget

PhishGuru

Comic to train people to spot phishing attacks

Best time to train is after a user has already fallen for an attack

Send out fake attacks and train those who click on them

Give users options that make sense and work for them

In Summary...

- Academics say in-the-moment training works
- Chief Security Officers (CSOs) have mixed opinions
- Everybody thinks that users clicking on links and attachments is a big problem

Passwords
Most recommended security behaviors

- 2/5 non-experts advice involves authentication
- 4/5 expert advice involves authentication

Passwords

- Most popular method of authentication
  - A character string (password) is agreed upon between the user and the system
  - User proves their identity by providing the password
- Convenient system design
  - Easy to store encrypted
  - Easy to enter on many systems
  - No special equipment needed
  - Scales well
- Problem: people choose easy to guess passwords
  - Low entropy, so easy to guess
  - Hard to remember

Passwords

- Most popular method of authentication
  - A character string (password) is agreed upon between the user and the system
  - User proves their identity by providing the password
- Convenient system design
  - Easy to store encrypted
  - Easy to enter on many systems
  - No special equipment needed
  - Scales well
- Problem: people choose easy to guess passwords
  - Low entropy, so easy to guess
  - Hard to remember

Standard password guidance

What does a good password look like?

- At least 8 characters, longer better
- No words (any language, especially English)
- Avoid common patterns
- Upper case letter as first letter
- Putting the number at the end
- Putting the special character at the end
- High entropy
- Lowercase letters
- Upper case letters
- Numbers
- Special characters

What does a bad password look like?

- Short
- Easy to guess (significant other attack)
- Uses common patterns
- Low entropy
- Word (in any language)
- Same combination other people use

UK guidance on simplifying passwords

1. Change all default passwords
2. Help users cope with password overload
3. Understand the limitations of user-generated passwords
4. Understand the limitations of machine generated passwords
5. Prioritize administrator and remote user accounts
6. Use account lockout and protective monitoring
7. Don’t store passwords as plain text

User generated passwords

- People are somewhat ok at generating passwords they can remember
- People are bad at generating passwords that are hard to guess
- User-generated passwords:
  - Low entropy
  - Tend to have facts about themselves such as their pet’s name
  - Guessable by someone who knows them
  - Easy to lookup in a password dictionary

PassFaces

- Humans are better at recognizing things than they are at recalling information.
- High feature information, like faces, are easier to recognize
- Idea: Use high feature information as the pin, so humans can recognize their password
- Problem: People select faces that mean something to them. If you know basic characteristics about someone you can easily guess their PassFace.

PassFaces

- Password length = 4
- Each password selected from a set of 9 faces like what is shown on the right
- Theoretical password space = 6561
- What is the best way to break someone’s password?
  - If the person is a white male, you can guess the correct password in about two guesses by selecting all the pretty white females.

Machine generated passwords

- Computers are better at selecting passwords that are challenging for other computers to guess
- Computers are less good at selecting passwords that are easy to remember
- Tactics:
  - Some algorithms produce passwords which are pronounceable, or are made up of words (correct battery horse staple)
  - Let users choose from a small number of passwords

Writing usable warnings

Why show warnings at all?

- Determined users might disable Safe Browsing. Which would prevent future warnings.
- User could also open the website in another browser that is less safe and does not block the website.
  - America Online users used to go to a friend's house to open malicious sites because the ISP blocked malicious sites.
  - Different browsers block different sets of sites, we don’t want to teach users to use less safe browsers.
NEAT and SPRUCE

- Developed at Microsoft Research
- Guidance on how to create effective security messaging for end users

NEAT

- Necessary – Can you change the architecture to eliminate or defer this user decision?
- Explained – Does your user experience present all the information the user needs to make this decision? (See SPRUCE)
- 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 user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team?

SPRUCE

- 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 they user makes the wrong decision
- Unique knowledge the 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 a decision

Questions