

Tabletop Experience:

The Password Guessing Game

Overview

Using weak passwords and oversharing on social media are two of the biggest security risks in modern security. Weak passwords increase the risk of unauthorised access to an organisation's network and sensitive data. Cybercriminals often utilise automated tools to guess login information in seconds. Once a bad actor gains access to an organisation's network, they can steal sensitive data, money or take control of systems.

This activity focuses on how attackers use publicly posted information to guess people's passwords or security questions. Participants will learn that even if a password isn't as obvious as '123456', personal details like pet names, birthdays or favourite sports teams make it easy for bad actors to break into accounts.

Roles

Facilitator:

Manages the pacing, guides discussions and ensures everyone participates.

Participants:

Discuss the ideas and respond to the scenario according to the exercise rules.

Introduction

Give the participants the scenario: Your team has been hired as 'ethical hackers' to test the security of a fictional department. You've identified an employee who is an active social media user. By looking through their public social media feed, your goal is to figure out their password before a real attacker does.

Part 1: Signs Annotation

 **Duration:** 15 minutes

Materials:

- Timer or stopwatch
- Scenario handouts
- Pens or pencils
- Paper sheets

Instructions:

- Divide the room into five groups.
- Hand out one persona to each group.
- Instruct groups to underline potential keywords, such as pet names, childhood streets, important dates and favourite hobbies.
- Direct groups to try and combine these keywords to 'crack' the person's password. Take into consideration symbols, numbers and special characters.
- Give the groups 15 minutes to read the posts, discuss and list their top five password guesses on the paper sheets.

Part 2: Discussion

 **Duration:** 10 minutes

The reveal:

Before starting the questions, the facilitator reveals the correct password for each persona and explains the logic behind it.

Questions:

- Which piece of shared information was the 'key' that made the password easy to guess?
- Did you find any 'false leads' – information the person shared that seemed like it would be a password but wasn't?
- How does it feel to see how much a stranger can learn about your habits just from a few posts?

Possible answers/prompts:

- **Oversharing:** Scammers look for life events (new car, new pet, graduation) because these are the words people most often use in passwords.
- **Password patterns:** Many people use predictable patterns (name + year) that are very easy to guess once you know their interests.
- **The core takeaway:** If a stranger can guess it, a computer can crack it in seconds. Personal information should never be part of your password.

Conclusion

 **Duration:** 5 minutes

Wrap up the exercise by connecting these concepts to your organisation's reality. Explain that while these characters were fictional, real cybercriminals use automated tools to do exactly what the participants just did manually – only much faster.

Take the opportunity to answer any questions that participants may have about creating strong passwords, protecting their accounts and practising safe online habits. Keep in mind these best practices:

- Use unique passwords for every account.
- Prioritise length over complexity when creating a new password. Try using passphrases – full sentences that work as strong passwords. They can contain spaces, special characters, numbers and other symbols. Example: *Bears! are eating yellow apples daily*
- Enable Multi-Factor Authentication (MFA) to secure your account. MFA adds a second verification step – like a mobile code, PIN or fingerprint – in addition to your strong password.
- Follow your organisation's policies on passwords.

Facilitator answer key

Persona 1: Sarah Miller

Answer: **Vegas2018!**

Sarah uses her hometown and graduation year. A simple search reveals the information a cybercriminal needs to break into her account.

Persona 2: Fatima Al-Sayed

Answer: **stargazerZin4**

Fatima uses her pet's name (Zina) and her hobby (stargazing). This is a 'behavioural warning sign' that shows how personal information is often used to create weak passwords.

Persona 3: Elena Rodriguez

Answer: **SophiaParis7**

Elena uses her daughter's name and age, mixed with a travel location. It may look good at first glance, but family members and travel information make the password vulnerable to criminal hackers.

Persona 4: Arjun Nair

Answer: **Arjun2004hatchback**

Arjun uses his first name and car information. It's a long password, but using your own name makes it extremely vulnerable. His nostalgia for the car is easy to find on his socials, making it a strong guess to discover his password.

Persona 5: David Chen

Answer: **Cooper_loves_hiking**

David uses his pet name and an activity they do together. It's a weak and obvious sentence that is easy to guess by scooping his socials – the underscores aren't enough to make it safe.

Attachment: Scenario handout part 1

Cut along the dashed line to create individual cards, providing one card to each group.

Persona 1



Sarah Miller

@sarah_miller

202 followers 125 following

Posts Replies Media



Sarah Miller @sarah_miller · 1d

Can't believe my best friend Bell is already 3 years old today! #PuppyBirthday



12 5 89



Sarah Miller @sarah_miller · 2d

Just bought my dream car! It's a bright blue Mustang. I've wanted one since I graduated in 2018.

1 12



Sarah Miller @sarah_miller · 3d

Check-in at Red Rock Canyon. So glad to be back in my hometown of Las Vegas!



1 5 5

Persona 2



Fatima Al-Sayed

@fatimaa

342 followers 392 following

Posts Replies Media



Fatima Al-Sayed @fatimaa · 1d

My cat, Zina, loves sitting on my blueprints while I work.



12 5 89



Fatima Al-Sayed @fatimaa · 2d

Spending the weekend stargazing at the Al-Qudra lake.

1 12



Fatima Al-Sayed @fatimaa · 3d

Beautiful sunset over the Jumeirah coastline tonight.



7 5 53



Attachment: Scenario handout part 2

Cut along the dashed line to create individual cards, providing one card to each group.

Persona 3



Elena Rodriguez

@erodriguez

445 followers 803 following

Posts Replies Media



Elena Rodriguez @erodriguez · 1d

Happy Birthday to my little princess, Sophia! Can't believe she's turning 7 today.



12 5 89



Elena Rodriguez @erodriguez · 2d

Finally visiting Paris! It's been my dream destination since I was a kid.

4 2



Elena Rodriguez @erodriguez · 3d

Morning routine: A double espresso and a walk on Maple Street. Best way to start the day!



1 1 4

Persona 4



Arjun Nair

@arjun_nair

645 followers 762 following

Posts Replies Media



Arjun Nair @arjun_nair · 1d

Watching the IPL finals tonight! Go Bangalore!



12 5 89



Arjun Nair @arjun_nair · 2d

Can't wait to see the Himalayas on my holiday next month!

3 2



Arjun Nair @arjun_nair · 3d

My first car was a 2004 blue hatchback. It survived so many trips!



1 5 5



Attachment: Scenario handout part 3

Cut along the dashed line to create individual cards, providing one card to each group.

Persona 5



David Chen

@david_chen

956 followers 243 following

Posts Replies Media



David Chen @david_chen · 1d

Cooper loved the hiking trail at Blue Ridge this weekend.



2 1 89



David Chen @david_chen · 2d

My first car was a 1992 silver saloon. I miss that car.

1 12



David Chen @david_chen · 3d

Watching the Lakers game – hope they pull off a win!



4 6 5

