

Making of: «Hack The Hacker»

<https://swit.ch/hack-the-hacker>

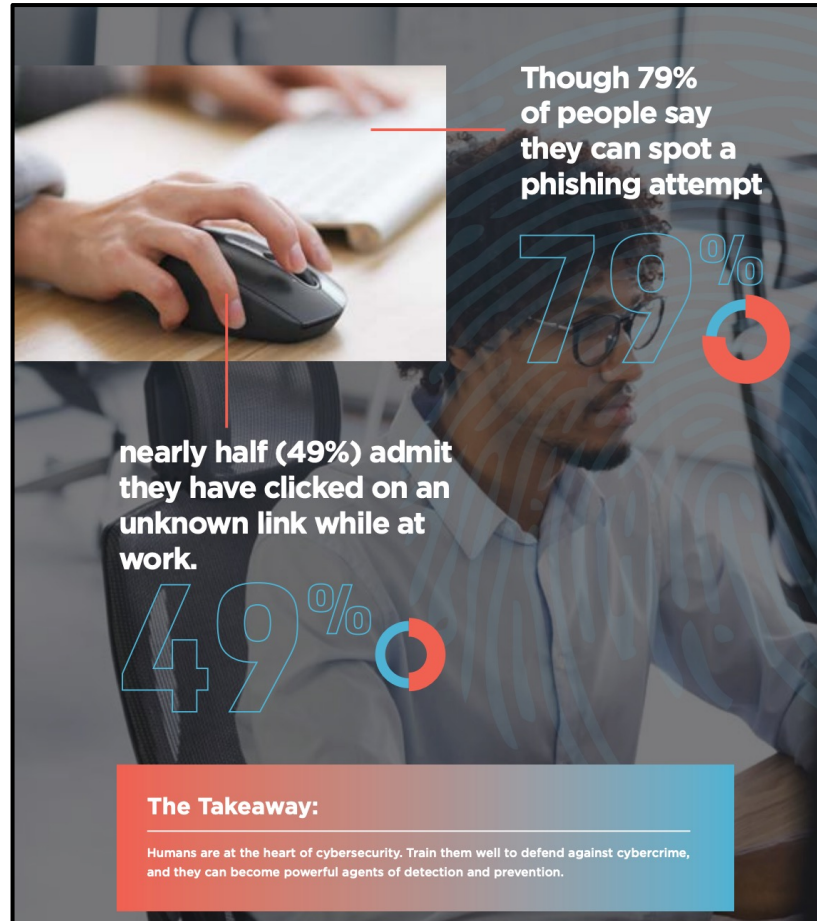
SWITCH

Oli Schacher & Fabio Greiner

awareness@switch.ch

#eduhubdays22





Livingsecurity 2020: 7 Essential Trends of Human Risk Management For 2021

What people say

91%

91% say they know using the same or a variation of the same password is a risk ...



80%

80% agree that having their passwords compromised is something they're concerned about ...



77%

77% say they are informed of password protection best practices ...



What people do

66%

... however, when creating passwords, 66% of respondents always or mostly use the same password or a variation – this is up 8% from our findings in 2018.

48%

... and yet 48% said if it's not required, they never change their password - which is up from 40% in 2018.

54%

... however 54% keep track of passwords by memorizing them





Gamification vs. Game Design

<https://en.wikipedia.org/wiki/Gamification>



https://en.wikipedia.org/wiki/Game_design



Advantage of Game Design in Trainings

Have some fun:

- Positive attitude
- Lasting learning effect through association with positive emotions

Freedom to fail:

- Approach a topic without fear
- Enables creativity

SWITCH Security Awareness Adventures



Escape Room

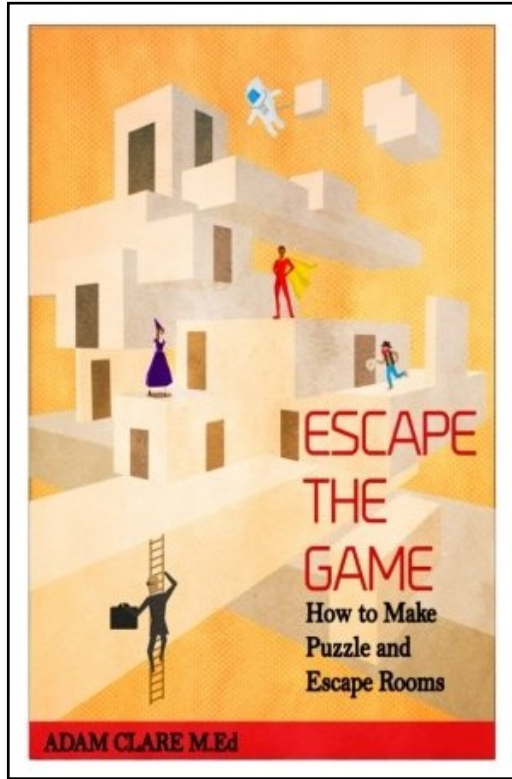


Scavenger Hunt



Dungeons & Dragons

Get the basics



Escape The Game

How to Make Puzzle and Escape Rooms

Adam Clare

CreateSpace Independent Publishing Platform 2016

Team building

Katja: Security Awareness, Communication

Jakob: IT-Security, Music

Andreas: IT-Security, Business

Antoine: IT-Security, Programming

Livia: Communication, Marketing

Oli: IT-Security, Games, Escape Rooms

Tipps:

- Interdisciplinary
- Team competencies determine opportunities
- Enthusiasm is everything!

Team building



Workshop

1. Security Awareness in a Escape Room
 - a. What is our goal?
 - b. Constraints / Requirements

Awarenes Topics

Phishing

Social Engineering

Dumpster Diving

Daten Backup

Ask the expert

Encryption

Password security

Malware / Virus

USB drives

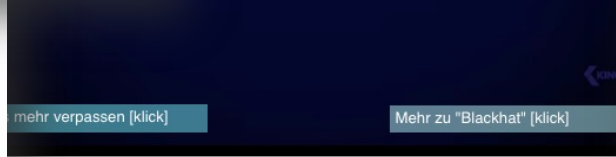
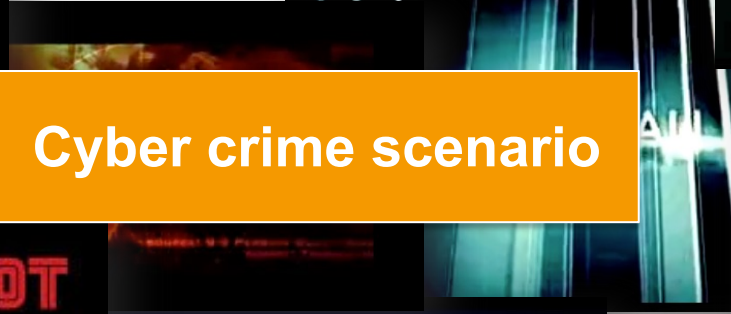
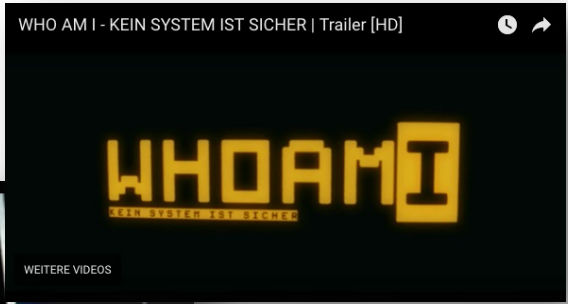
Guiding theme



Cyber crime scenario

Ransomware attack

untraceable



cyber crime



Inspiration / Color palette

hacker



ransomware



10 Dinge für Themenwelt

1. Computer
2. leere Chipstüte im Müll
Redbull-Dosen, Pizzaschachteln
3. Poster (hacker film, game)
4. Printouts (z.B. Phrack-magazine)
5. Hoodie
6. blinkende LEDs (SWITCH,
get it?)
7. elektroschrott (USB-Festplatte,
Kabel, webcam,
Handy)
8. Safe mit Zahlenschloss
9. Rubiks Cube
10. Guy Fawkes (Anonymous)
Maske

Start

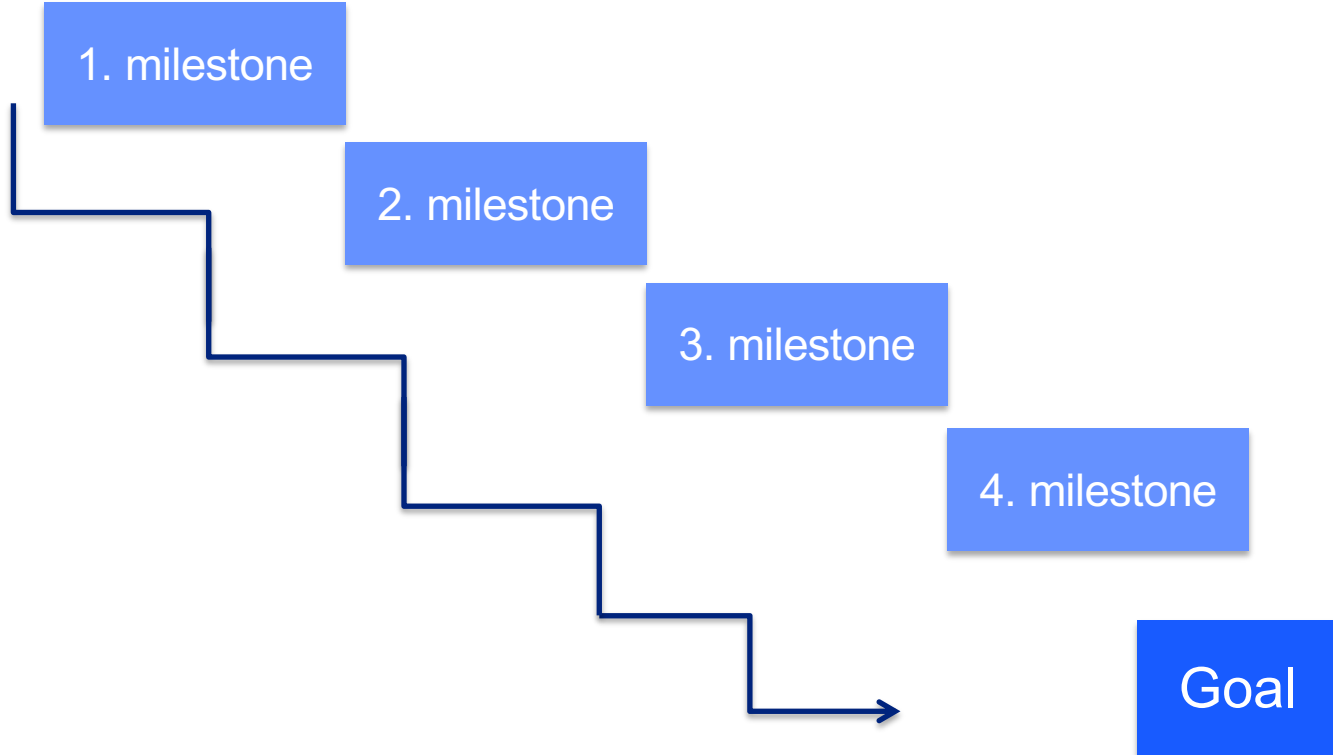
Storyline

Goal



Start

Storyline



Start

Storyline

1. milestone

Puzzle
Puzzle

2. milestone

Puzzle
Puzzle

3. milestone

Puzzle
Puzzle

4. milestone

Puzzle
Puzzle

Goal

Puzzles

- **Logic puzzles**
Search for patterns, similarities, ...
- **Codes, Crypto**
Encrypted text, calculate numbers
- **Combined puzzles**
In order to solve puzzle B you need the solution from puzzle A
- **Scavenge hunt, path finder**
Follow arrows, find path with a map, ...
- **Teamwork**
Someone reads manual while the others execute, press buttons at the same time, ...
- **Hidden things**
Hide clues, sometimes in plain sight...

Puzzles: Immersion & The awesome moment



```
Approaching final keyspace - workload adjusted.
```

```
Session.....: hashcat  
Status.....: Exhausted  
Hash.Name.....: MD5  
Hash.Target.....: hashes.txt  
Time.Started.....: Tue Sep 14 17:50:02 2021 (0 secs)  
Time.Estimated...: Tue Sep 14 17:50:02 2021 (0 secs)  
Guess.Base.....: File (/usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 3714.1 kH/s (0.18ms) @ Accel:1024 Loops:1 Thr:1 Vec:8  
Recovered.....: 5/6 (83.33%) Digests  
Progress.....: 10003/10003 (100.00%)  
Rejected.....: 0/10003 (0.00%)  
Restore.Point....: 10003/10003 (100.00%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1  
Candidates.#1....: beckyl -> telegram
```

```
Started: Tue Sep 14 17:49:46 2021  
Stopped: Tue Sep 14 17:50:04 2021
```

```
(kali@kali)-[~]  
└─$
```

Material



Transport-Koffer
Polaroid plus Film
Hacker Laptop
Victim Laptop
Baby Phone/Kamera
Safe
Poster
LEDs
Festplatte
Funkgeräte
Alukoffer
Bücher
Raspberry Pi
Raspberry Pi Zubehör
Lautsprecher
Rubiks Cube
Hoodie
USB Stick
Steckerleiste
Adapter
Schreibtischlampe
Box + Kette
Mouse
Schloss (Master Lock)
Laptop-Sticker
Cyber Absperrband und Aufkleber
alte T-Shirts/Hosen/Schuhe
Geldbeutel
Postits, Schreiber, Schere, Klebeband
UV-Neon Stift
Gummibärchen
Kasse
Maske
Pizzaschachteln
"Müll"
ASCII-Tabelle
Hacker Polaroid
Ausweise
Anleitungen/Artikel
Sticker Rubiks Cube
Batterien
Safe Dose

Finding a room





Test, adapt, document

Escape Room für SWITCHIES

Freitag, 07. September 2018 [Jakob Dhondt](#)

Hoi Zäme!

Damit jeder einmal den bösen Hacker überlisten kann, haben wir vier Termine erstellt, an denen, wer möchte, den Escape Room selbst einmal erleben kann. Pro Termin können maximal fünf Teilnehmer mitmachen. Tragt euch bei Interesse einfach in folgendes Doodle ein! <https://doodle.com/poll/9s2d4b8nuvu7b7qe>

Und unbedingt den [Trailer](#) anschauen!

Liebe Grüße,

Euer Escape Room Team



15 min



30 min



45 min



60 min



We're ready to go!

...or are we?

Running Hack the Hacker

- It's no longer a project, its a service
- We didn't plan, because people have other things to do
- Outsourcing? Security knowledge is important
 - Always 2 people (techie/non-techie)




Running Hack the Hacker

- Intro/Briefing/Teaching

Ransomware

My documents
and photos
are important
to me!




Meine Daten
und Fotos
sind mir sehr
wichtig.

plain text

cipher text

© 2021 SWITCH | 33



1. Security-Einstellungen prüfen
2. Profilsichtbarkeit beschränken
3. Sparsam mit Daten umgehen

Running Hack the Hacker

- Intro/Briefing/Teaching
- **Game**



Running Hack the Hacker

- Intro/Briefing/Teaching
- **Game**

T-50 min: Solved puzzle 1

- Tip 1
- Tip 2

T-40 min: Solved puzzle 2

- Tip 1
- Tip 2
- Tip 3

T-25 min / T-10 min: Solved puzzle 3 or 4

Puzzle 3

- Tip 1
- Tip 2

Puzzle 4

- Tip 1
- Tip 2

T-5 min: Solved all the puzzles

Running Hack the Hacker

- Intro/Briefing/Teaching
- Game
- Debriefing

Hack The Hacker – tips

Recommendations for hacker-hackers



RANSOMWARE
It is malware that encrypts all the data on your computer. The attacker blackmails you by demanding money for the decryption code.

Talk to experts
Your computer is infected with ransomware, talk about the type of malware being used, the decryption code is already available, you can benefit from specific tips.

Don't pay
Due to the demands of criminal hackers if your computer is infected with ransomware. It's not that you'll get your data back if you do, but by supporting a criminal system.

Regular backups
Regular backups will suffice to protect yourself from the most significant consequences of a infection, and will also help if you use a ransomware or break your device.

PASSWORDS
Using a password is key to protecting your (personal) data.

Choose unique passwords
If a hacker has gained access to one of your passwords, they'll test it quickly and automatically to see whether it can be used to access other online platforms. Never use a password more than once.

SWITCH

RANSOMWARE
It is malware that encrypts all the data on your computer. The attacker blackmails you by demanding money for the decryption code.

Talk to experts
Your computer is infected with ransomware, talk about the type of malware being used, the decryption code is already available, you can benefit from specific tips.

Don't pay
Due to the demands of criminal hackers if your computer is infected with ransomware. It's not that you'll get your data back if you do, but by supporting a criminal system.

Regular backups
Regular backups will suffice to protect yourself from the most significant consequences of a infection, and will also help if you use a ransomware or break your device.

PASSWORDS
Using a password is key to protecting your (personal) data.

Choose unique passwords
If a hacker has gained access to one of your passwords, they'll test it quickly and automatically to see whether it can be used to access other online platforms. Never use a password more than once.

Use min. 14 characters (uppercase, lowercase, special characters and numbers)
It takes less than two minutes to crack a five-character password made up entirely of lowercase letters. The longer and more complicated a password is, the less likely it is to be cracked.

Choose two-factor authentication (2FA)
Many online services offer the option of logging in using two-factor authentication (2FA). Activate this option whenever possible.

What is a password hash?
In order to store passwords as securely as possible, a hash function is used to transform the plain text into a hash value. When a password is entered, the same hash function is used to calculate its hash value and compare it with the one stored. If the password hash is the same, the password is correct.

SOCIAL ENGINEERING
Black hats don't just hack computers, they also hack people. This method is known as social engineering. Using psychological tricks, they attempt to gain information via email, phone or in person.

Take a step back
Don't allow yourself to be put under pressure. Don't tell anyone else your passwords. Don't discuss internal matters with anyone who isn't involved. If you're not sure, ask – clarify the sender/your counterpart's identity and permissions.

Really check
If an offer seems too good to be true, it's worth being a little suspicious. Look for references for the website making the offer or verify the existence of the competition you're won.

Query it
In general, if something seems off, query it over a different communication channel to make sure.

SWITCH



Running Hack the Hacker

- 13:00 Prepare escape room and presentation room
- 14:00 Welcome the participants and game introduction
- 14:30 Start of game
- 15:30 End of game / Debriefing
- 16:00 Reset room and stow material
- 16:30 Done

Total time: 3.5h, two people



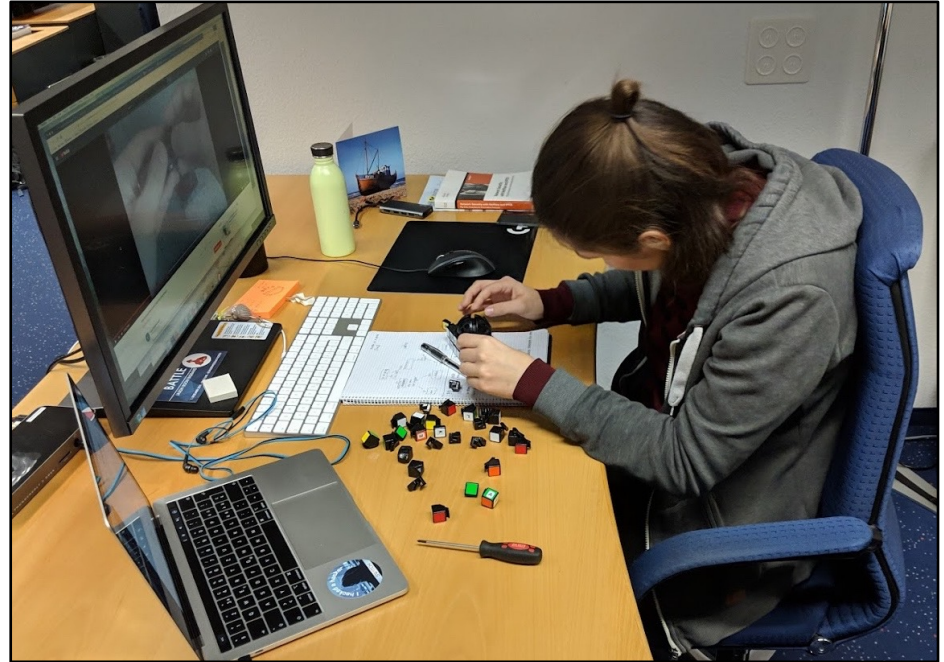
Challenge: Time management

Challenge: Participants often want to stay and know more

- Main goal reached!
- At the same time difficult, when next group is planned
- Time needed to reset
- Important to have solid learning points implemented
- Focus on the goal



Challenge: Unforeseen problems



Challenge: Maintenance

- Software components
- Important objects not available anymore

Challenge: Marketing

SWITCH Services - Stories - About us -

SWITCH-CERT For Universities For Banks For Industry & Logistics Info-Desk Contact / RFC 2350

«Hack The Hacker» - The SWITCH Security Awareness Experience

A criminal hacker has infected the computer system of your organization with ransomware. All data is encrypted. Your team has to outwit the hacker and rescue the data. Will you discover the decryption code?

Gain the knowledge. Face the threat. Hack The Hacker.

Hack The Hacker - The SWITCH Security Awareness Experience
SWITCH Security Videos

Criminal hackers count on you to threaten your organization.

A training to remember

Scenario Concept Security Awareness topics

Ransomware in your organization

A click on a link in an email infects the computer system of your organization with ransomware. It's up to you and your colleagues to rescue the data. You have to put down the attack of the criminal hacker.

The mission of your team is to discover the code that revokes the encryption executed by the malicious software. Together with up to 6 people you have to search the hacker's den for hidden hints and clues.

In order to find them and to solve all the puzzles you have to turn into hackers yourselves. Outwit the hacker and save your organization!

Info-Desk
Public DNS
Security Awareness
Hack The Hacker
SWITCH-CERT Report
Security Reports
Papers & Presentations
Security-Blog & Twitter

Hack The Hacker

Duration: ca. 2 h
Number of participants: max. 6 pers.
Target group: employees of all fields, students
Location: SWITCH Werdstrasse 2 8004 Zurich
Price: on request

"Hack The Hacker" - Flyer

NO MORE RANSOM!

The website "No More Ransom!" helps victims of ransomware decrypting the data without paying the ransom to the criminals.

<https://www.nomoreransom.org/>

<https://swit.ch/hack-the-hacker>

What is ransomware?

Ransomware is malware that encrypts all the data on the infected computer. Without the correct decryption code the data is lost. The attacker is making money out of it, through blackmailing the data owner: money in exchange for the code.

It is advised not to pay the ransom because there is no guarantee for getting back the data.

Between April 2016 and March 2017 more than 2.5 Mio. users have been confronted with ransomware. 2017 every second company was affected. The average damage per organization adds up to around CHF 123'000 per case.

SWITCH-CERT Security Awareness

Katja Dörlemann
Awareness Specialist
+41 44 268 16 42

More Hacker-tainment

Movies and Series Books Games Fun

TV shows

Mr. Robot
IT Crowd

Movies

Matrix
Snowden
Who am I - Kein System ist sicher
Swordfish
Hackers
Three Days of the Condor
WarGames



What we **can** do with Hack The Hacker

- Raise (longterm) interest in security
- Encourage users to deal with IT related topics
- Improve the reputation of the security department
- Improve teamwork



What we **can't** do with Hack The Hacker

- Train a high number of employees in a cost-effective way
- Optimise it to a cost-effective training tool
- Quickly adapt to new topics



4 Learnings

1 Development is one thing, implementation is another:

When? Who? How long? How many?

2 What can be broken, will be broken:

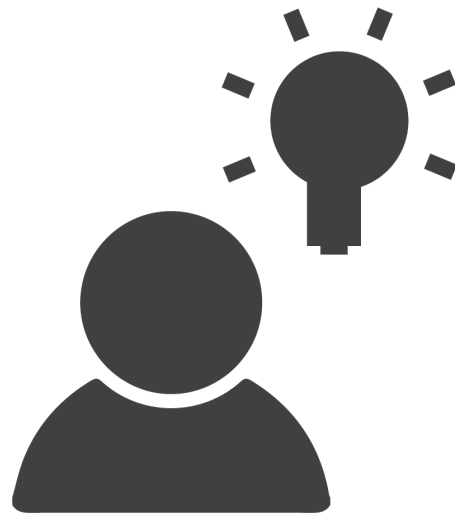
Stock of material, adapt budget (Rubik's Cube!)

3 Don't forget the time to reset:

Take time for set up and set down

4 Sweets protect against frustration:

Celebrate achievements and mark dead ends



SWITCH

