

# Ethical Student Hackers

---

Lock picking



# The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.
- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.
- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.
- Relevant UK Law: <https://www.legislation.gov.uk/ukpga/1990/18/contents>



# Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.
- If you have any doubts or need anything clarified, please ask a member of the committee.
- Breaching the Code of Conduct = immediate ejection and further consequences.
- Code of Conduct can be found at  
<https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf>



# Lock picking Risks and Law

Similar to normal more digital sessions the skills you'll be learning can be misused. However there are some slightly different points:

- Only pick society locks or your own locks
  - Criminal Damage Act 1971 <https://www.legislation.gov.uk/ukpga/1971/48>
  - Penalties for purely misuse of lockpicking tools (not including unauthorized entry or damage to property)
    - Fines (Up to £5,000)
    - Community Service
    - Imprisonment (Up to 5 years, depending on severity)
- Follow the instructions given and use minimal force to prevent injury. Let someone on the committee know immediately if you do hurt yourself.
- Everyone must sign the sheet to acknowledge you are here and have seen these rules (required by SU to do this)

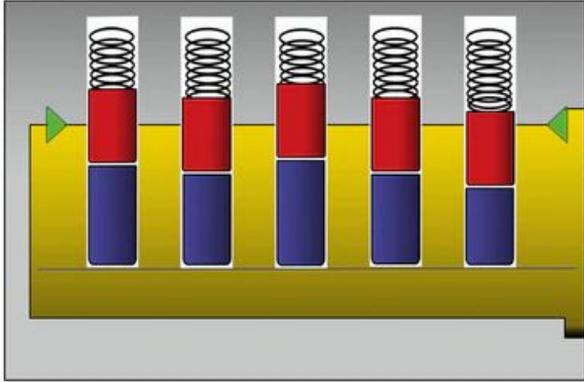


# Why is lock picking useful?

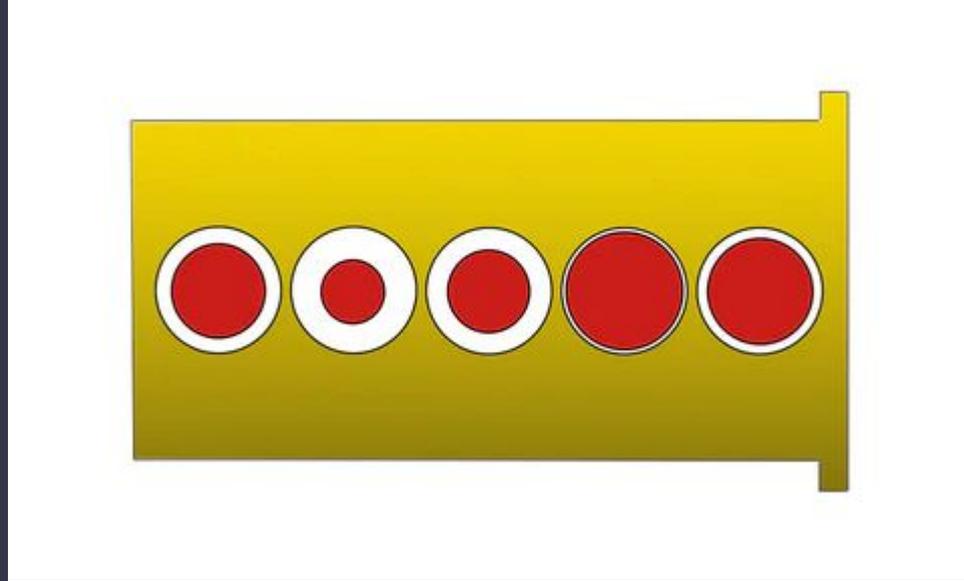
- What makes hacking 'ethical'
- What if we can't hack the client?
- Pen testing
- Most devices will give you almost complete access if you are physically there
  - Factory reset button
  - Device management
  - USB access (air gapped stuff)



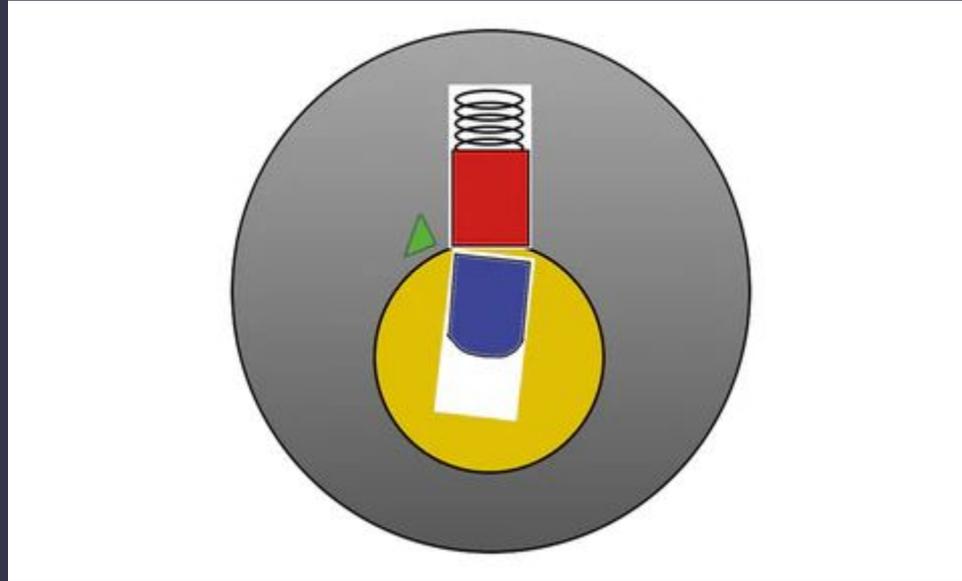
# Single pin picking



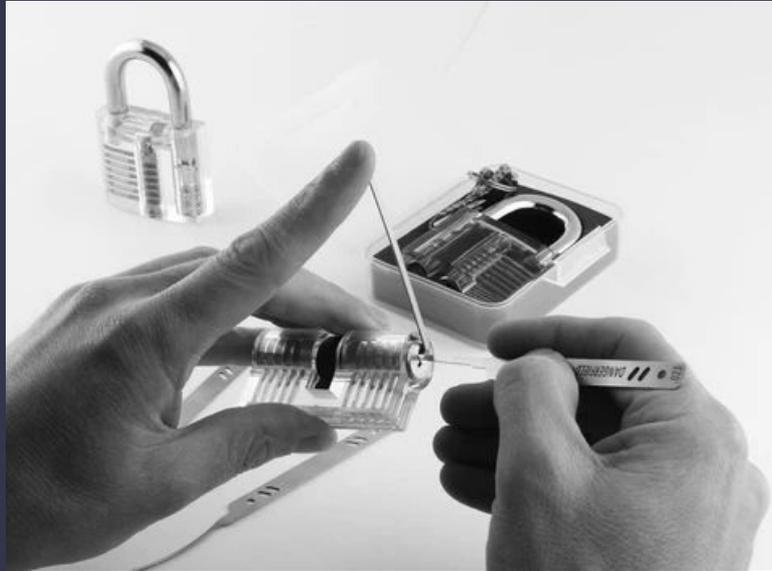
# Single pin picking



# Single pin picking



# Single pin picking



# Upcoming Sessions

What's up next?

[www.shefesh.com/sessions](http://www.shefesh.com/sessions)

Heavily inspired by:

- <https://www.lockpickworld.com/pages/how-to-pick-locks>
- How to Pick Lock: A Definitive Guide to Single-Pin Picking | Chris Dangerfield

Special thanks to:

- Hagen Locksmiths

# Any Questions?



[www.shefesh.com](http://www.shefesh.com)  
Thanks for coming!

