



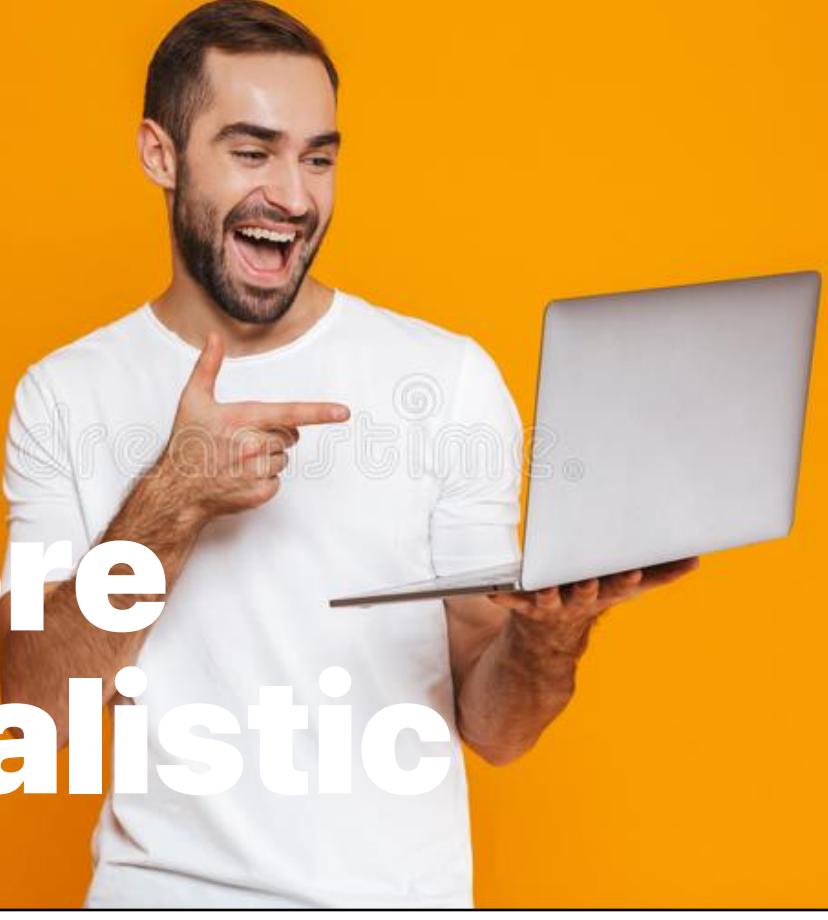
# Hacking



How do you  
think hacking  
works?



# Myth



A man with a beard and short hair, wearing a white t-shirt, is laughing heartily with his mouth wide open. He is pointing his right index finger towards the screen of a silver laptop he is holding in his left hand. The background is a solid orange color. A faint watermark "Dreamstime" with a registered trademark symbol is visible in the center of the image.

# More Realistic



**Even more  
Realistic**

# **Hacking**

**Abuse the intended  
behaviour to your  
benefit**

# Level: Easy



# Level: Not Hard enough

Universität Duisburg-Essen

Offen im Denken

Infos für... ▾

Einrichtungen ▾

Fakultäten ▾

Medienkontakt

Digitale Dienste der UDE derzeit nicht verfügbar



(Bild: mhphotodesign – stock.adobe.com)

# Level: Hard





# Ransomware



# Never pay the ransom



We hold the world ransom for...

**You don't  
know that  
they will send  
you the key**

**You will fuel  
their  
practise**



# Hacking: Theory

HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.

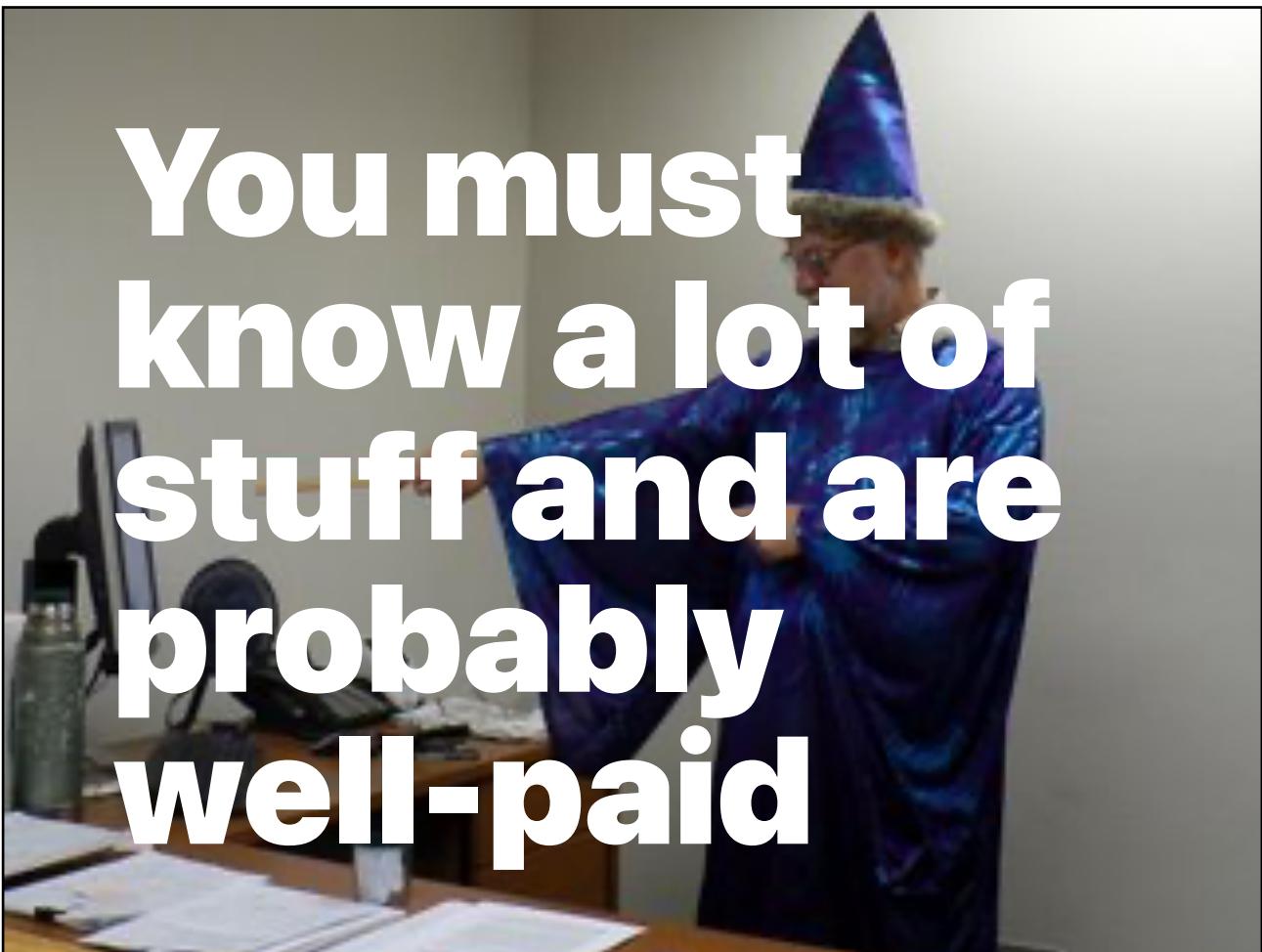
HI BOB! HOW CAN I HELP YOU TODAY?

# Hacking: Practise

# Theory (Hard): Puzzle

- Which ports are open?
- What services are running?
- Do they have known CVEs?
- Do I know users that have access?
- Do they have known passwords from leaks?
- Can I fuzz the password?
- How do I get a backdoor

You must  
know a lot of  
stuff and are  
probably  
well-paid



# Practise (Easy): Find idiots

- Who has access to important nodes?
- Can I get them to share their credentials with me?
- Can I get them to plug in my USB drive?
- Can I send them an executable that they run?
- Can I just ask them to use their computer?
- Can I just access their computer after office hours?

**Computers  
can be  
controlled,  
people not**



# Phishing

# The "does it work for you?"

Hi,

Hast du auch Probleme dich hier anzumelden?

1)<http://www.uni-due.examinationoffice.com>

LG Silke

**URLs are weird**

**[http://activate.facebook.fblogins.net/  
88adba079828308298398?  
login.asp](http://activate.facebook.fblogins.net/88adba079828308298398?login.asp)**

**<http://www.cnn.com/tiger-woods/story.html>**

**<http://www.buy.com.money.ru>**

**<ftp://ftp.microsoft.com/software/patches/fixit.exe>**

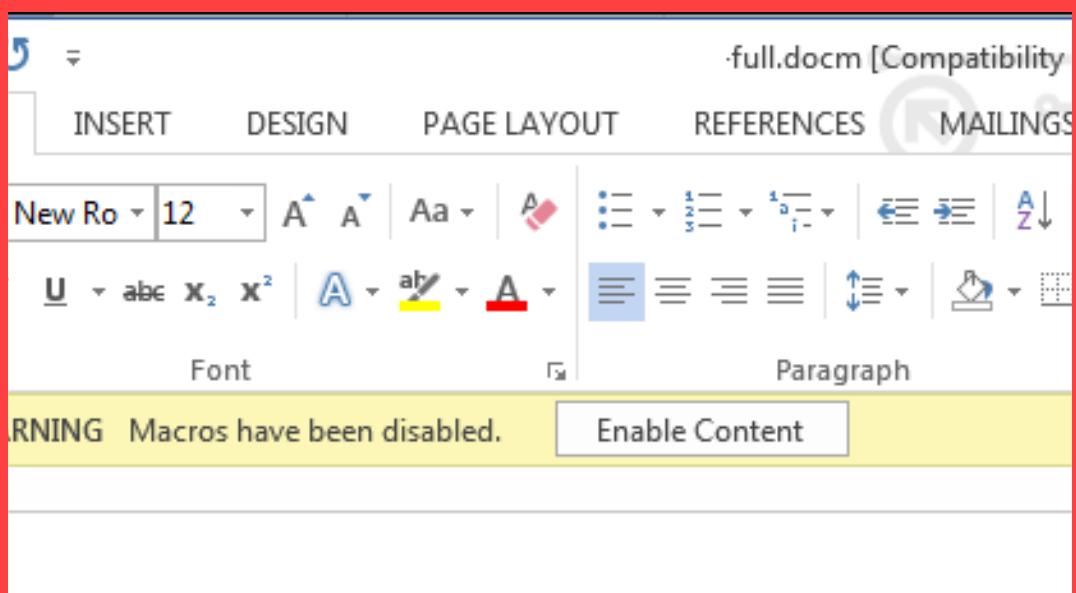
**<http://www.micosoft.com/software/patches/fixit.exe>**

**Try for yourself!**  
**[https://robinagandhi.github.io/phishing-  
demo/phishing.html](https://robinagandhi.github.io/phishing-demo/phishing.html)**



# USB Drops

# Makros



# Idiot Employees



**Hacker got  
access,  
what's so  
bad now?**

# **Government/Spy Agency**

- Sit back
- Stay stealthy
- Gather intel
- Victim mustn't know it's being spied on!

# Blackhat

- Get credit card/payment info
- Get passwords to money accounts
- 2FA etc. made this less lucrative
- Get sensible information for blackmail
- Encrypt files for ransom
- Install backdoor and come back to hack other devices in the network

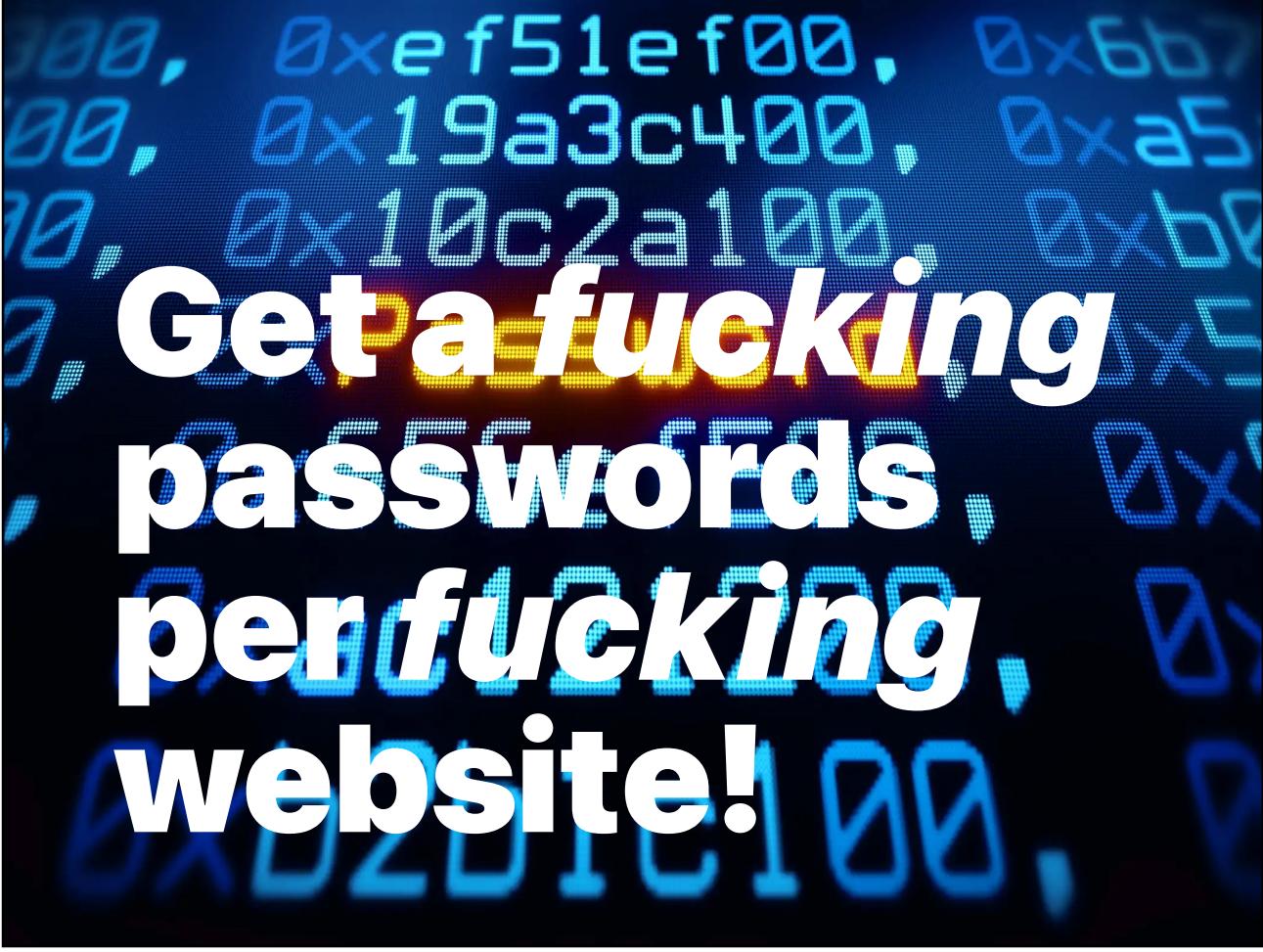
**How to  
prevent/mitigate  
damage?**



**Update your  
software!**



Access  
control!



Get a fucking  
passwords,  
per fucking,  
website!



– Backup: Arkonis

**Assume  
something  
went wrong,  
how bad  
would it be?**