



Hackable me

On cybercrime
and hacking



Steve Muller

What is “hacking”?



“hacking means exploring the limits of what is possible, in a spirit of playful cleverness”

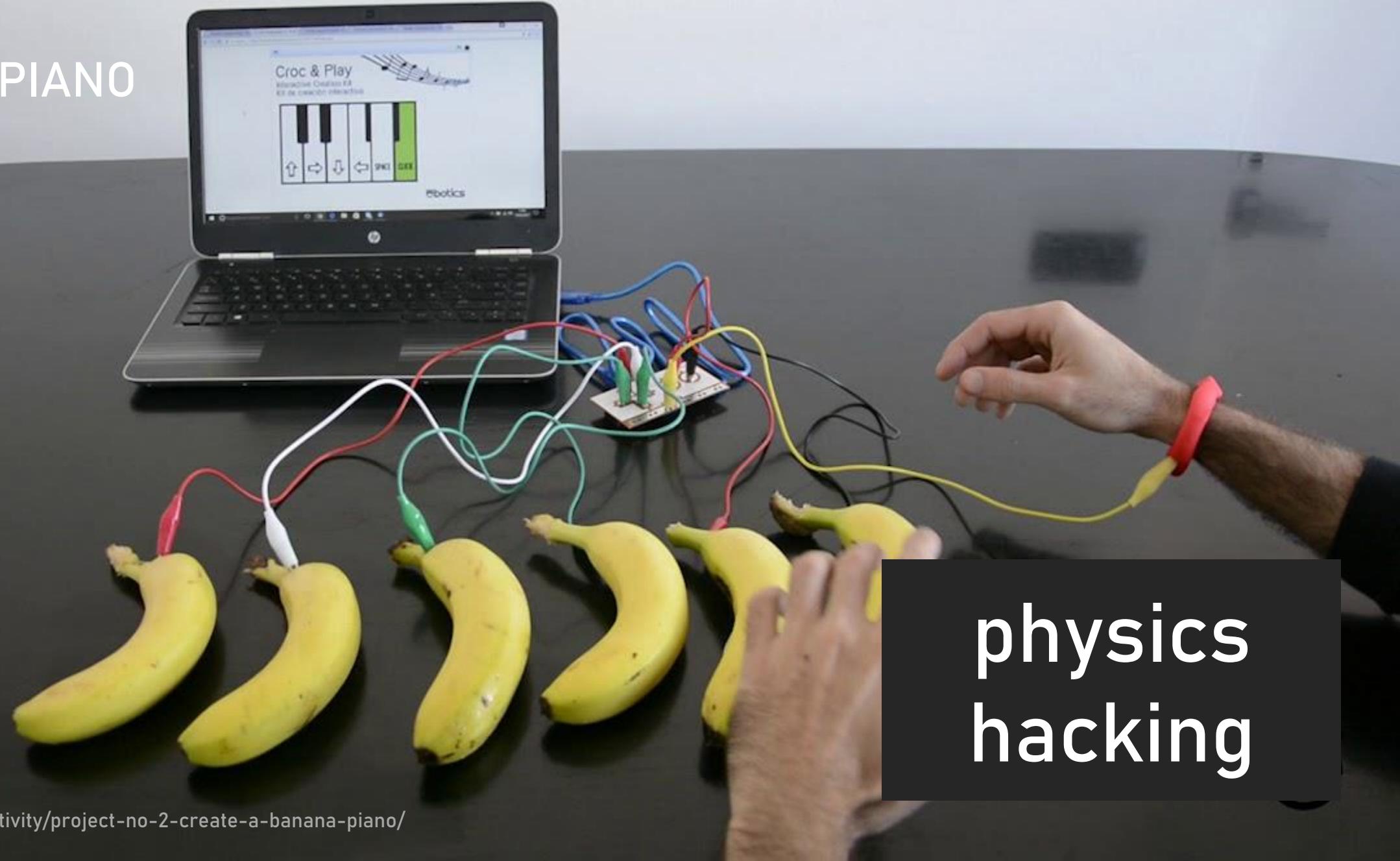
– Richard Stallman

Father of the free software movement

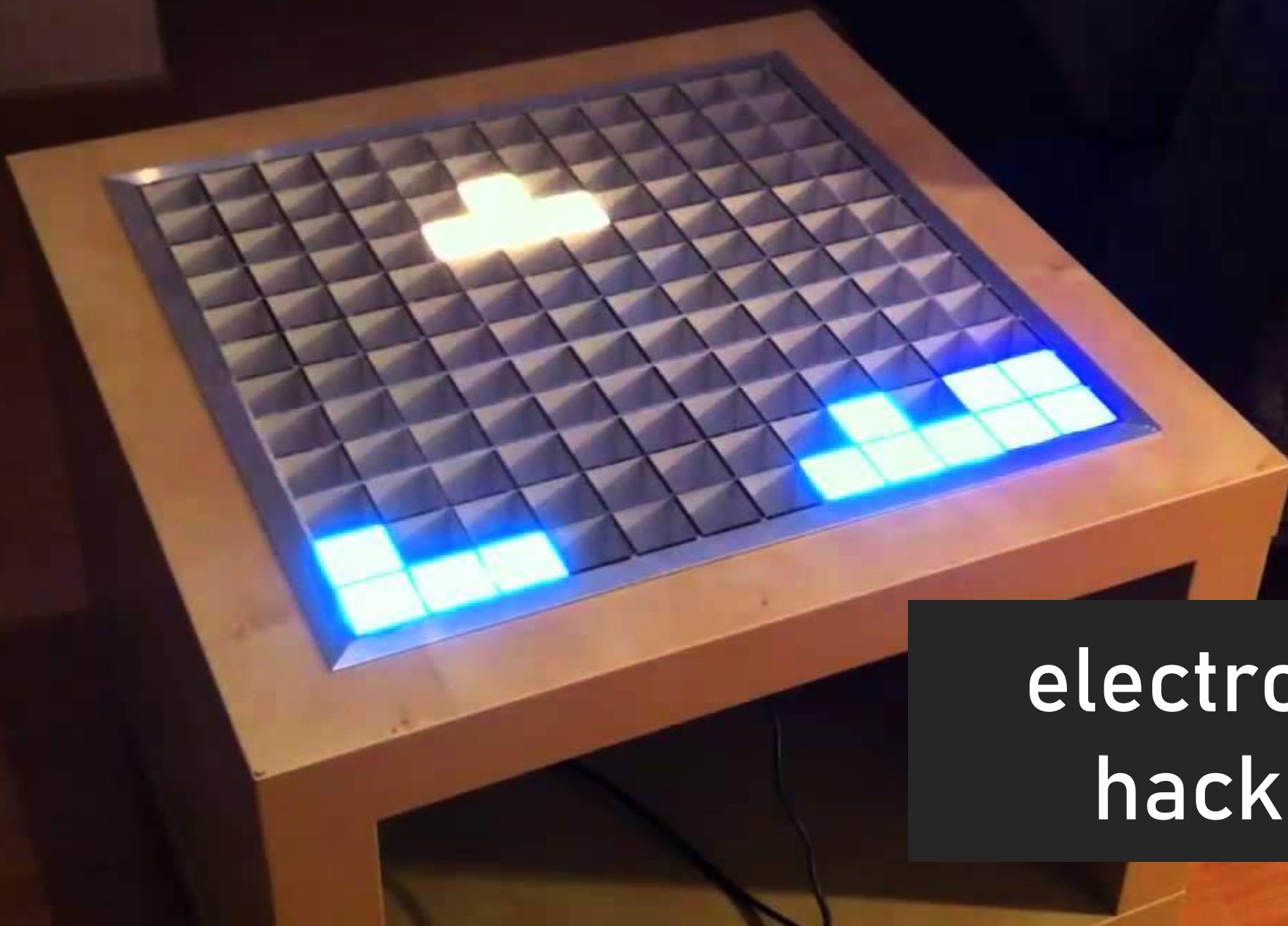


Furniture hacking

BANANA PIANO



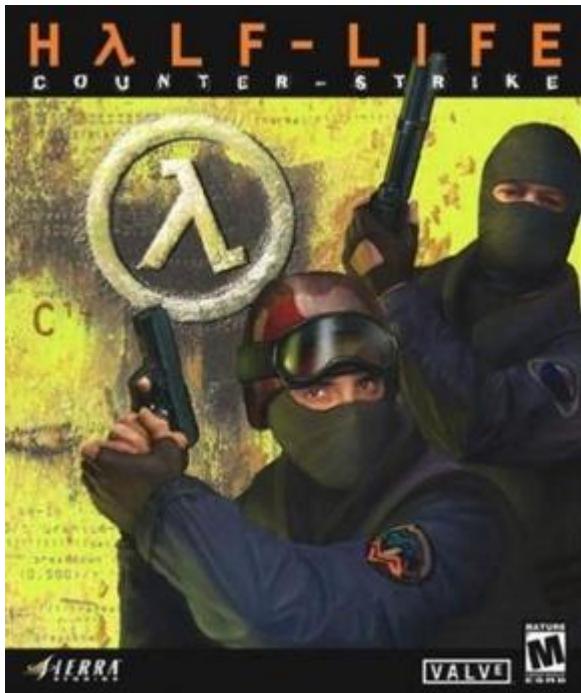
physics
hacking



electronics
hacking

Hacking in IT:

Make computer programs do things
that were not originally intended



Counter strike (1999),
originally a mod of the popular
shooter game “Half-Life”

2023:
(still) Top selling
game on Steam



A screenshot of a NoCry ransomware decryption interface. It features a large red "NoCry Decryptor" logo with a padlock icon. The main message reads "Ooooops All Your Files Are Encrypted ,NoCry". Below it, a question "Can I Recover My Files ?" is followed by a response "Yes, You Can Recover All Your Files Easily And Quickly". A section titled "But How ?" contains the instruction "Send The Required Amount And I Will Send The Key To You For Decryption". A timer shows "71 : 58". The message "See You Soon (0_0)" is displayed. At the bottom, there's a "bitcoin" logo and a copyable address: 1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK. Buttons for "About bitcoin", "How to buy bitcoins?", "Contact Us", "Show Encrypted Files", and "Decrypt" are also present.

ETHICAL HACKING

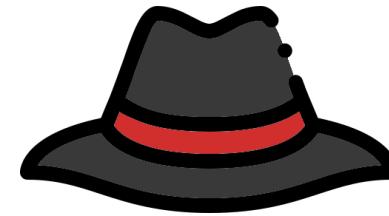


“white hat”
hackers

UNETHICAL / CRIMINAL HACKING



“gray hat”
hackers



“black hat”
hackers

good means

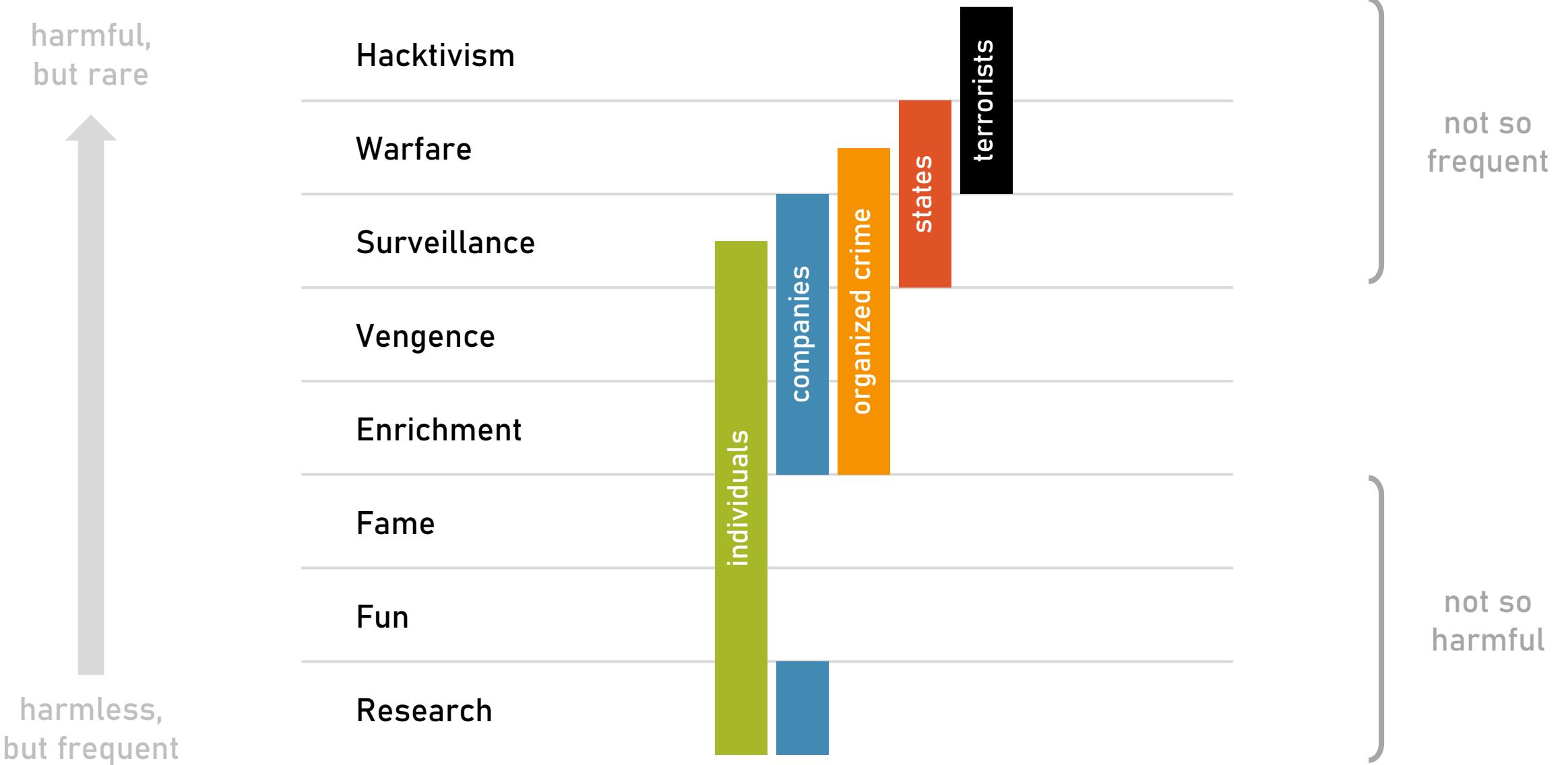
bad means

good intentions

bad intentions

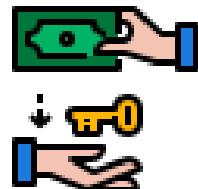
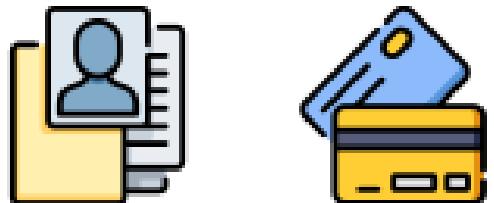
HACKING

Motivations to hack

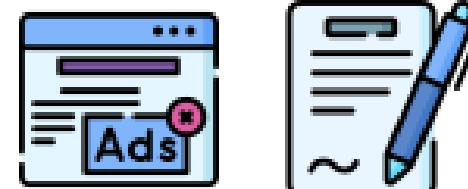


Cybercriminals are after ...

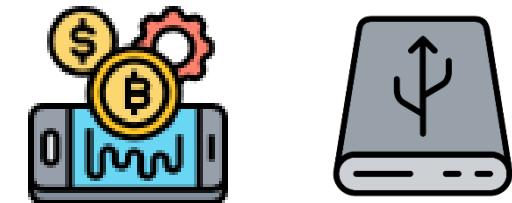
your
data



your
identity



your
resources



DARK MARKETS

ESCROW Order ixigo ESCROW Order

[Round 2] 4 million+ roll20.net Accs [Round 2] Petflow 1m md5 & various vb forums

B0.0584 gnosticplayers (5.0) WW O

Vendor: pinkcard Sales: (475)
Last seen: Today

Always stay safe!
You are Escrow protected for each product in the market! Never pay down a deposit in another vendor address.

REGULAR CREDIT AND DEBIT CARDS WITH UNKNOWN BALANCE FRESH
100% GUARANTEED

Product quality ★★★★★
Product type Digital
Quantity sold
Quantity left

Pay with Type
BTC XMR Normal Escrow

Please select an offer
1 item for 23.00 \$

1 + Add to cart Report

B0.178

[Round 2] Coinmama Database

B0.0584 gnosticplayers (5.0) WW O

Show product images

Coinmama ESCROW

[Round 2] StrongHoldKingdoms (Gaming / 5M+)

B0.

Personal
data (U.S.)

\$4

Personal
data (EU)

\$80

Scanned
passport

\$65

1 hour attack
denial-of-service

\$25

Facebook
login

\$9

Access to
compromised PC

\$26

Sources: "Pricing Analysis of Goods in Cybercrime Communities". *Flashpoint*. Oct 2019.
"Average price of stolen credentials on dark web marketplaces". *Statista*. Feb 2019.

Cybercriminals are after ...

your
data



your
identity



your
resources



“HACKING”



LastPass Security Notice ➤ Inbox x

 LastPass <LastPass@secure-monitor.com>
to me ▾

LastPass****

Dear LastPass User,

We wanted to alert you that, recently, our team discovered and immediately blocked suspicious activity on our network. Some user vault data was taken including email addresses and passwords.

To be sure that your information was NOT compromised, we have built [this secure web site](#) where you can enter your last pass login information and we can tell you if your account was one that was compromised.

We apologize for the inconvenience, but ultimately we believe this will better protect LastPass users. Thank you for your understanding, and for using LastPass.

Regards,
The LastPass Team

[Learn More](#)

can't they
“hack”
or fake the
sender
address?

Theoretically yes, although there are security restrictions like SPF, DMARC, DKIM and bla bla bla bla

but heck yes THEY CAN

but why should they?
when people fall for **this**

Cybercriminals are after ...

your
data



your
identity



your
resources



“HACKING”

OF PEOPLE

“social engineering”

“HACKING”

OF PEOPLE

fear (fake) “Sextortion”

Von: Beitris Englert <hbeleonoretvi@outlook.com>

Datum: 12. Juli 2022

Betreff: Ech hunn dech opgeholle

Et schéngt, datt PeterLustig123 Äert Passwuert ass. Dir kennt mech vläicht net an Dir frot Iech wahrscheinlech firwat kritt Dir dës E-Mail, richteg?

Tatsächlech hunn ech e Malware op der Erwuessene Videos (Porno) Websäit opgeriicht a roden wat, Dir hutt dëse Site besicht fir vill Spaass (Dir wësst wat ech mengen). Wärend Dir Videoe gekuckt hutt, huet Ären Internetbrowser ugefaang fonctionnéiert als RDP (Remote Desktop) mat engem Keylogger deen mir Accessibilitéit fir Är Écran an Web Cam. duerno, meng Software Programm kritt all Är Kontakter aus Är Messenger, FB, souwéi E-Mail.

Wat hunn ech gemaach?

Ech hunn en duebel-Écran Video erstallt. Den 1. Deel weist de Video deen Dir gekuckt hutt (Dir hutt eng gutt schmaacht haha ...), an den 2ten Deel weist den Opnahm vun denger Webcam.

genee wat soll Dir maachen?

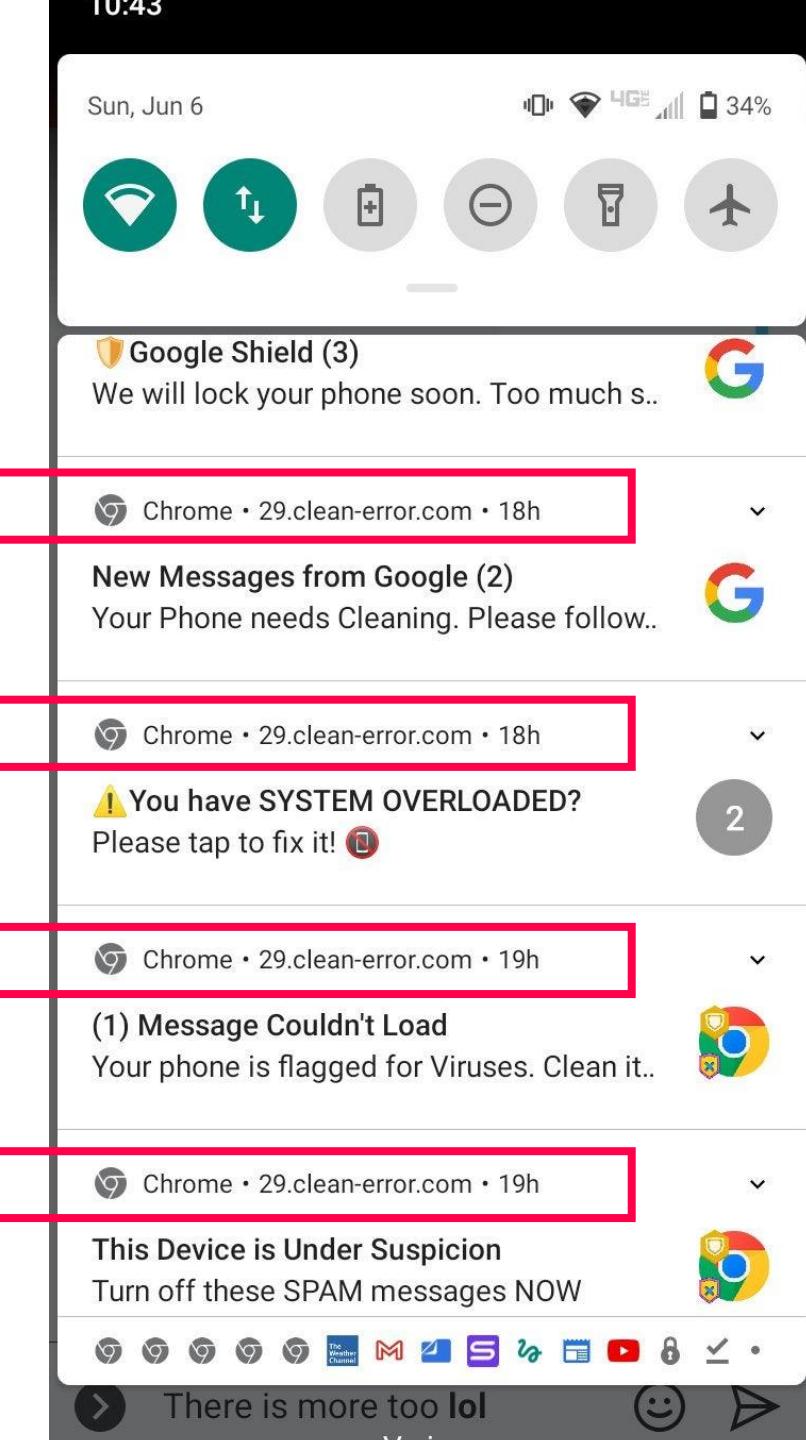
Gutt, menger Meenung no, \$2900 ass e faire Préis fir eist klengt Geheimnis. Dir maacht d'Bezuelung mat Bitcoin (wann Dir wësst dat net, sicht "wéi Bitcoin ze kafen" op Google).

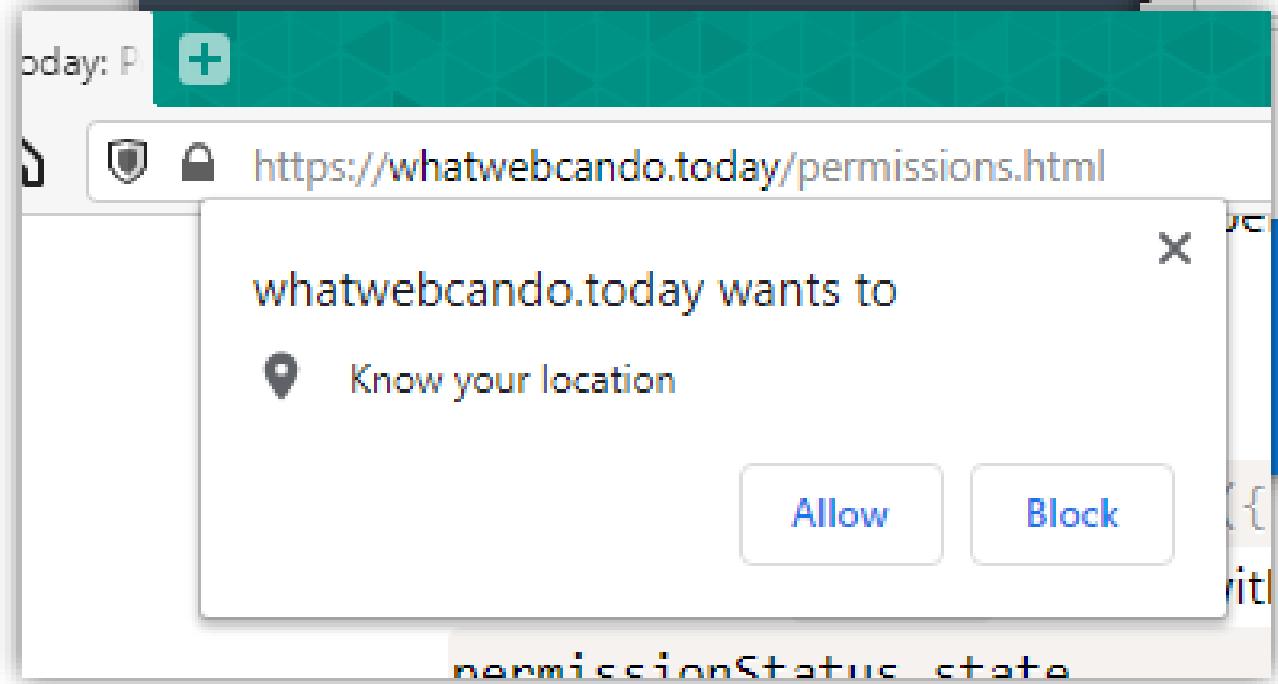
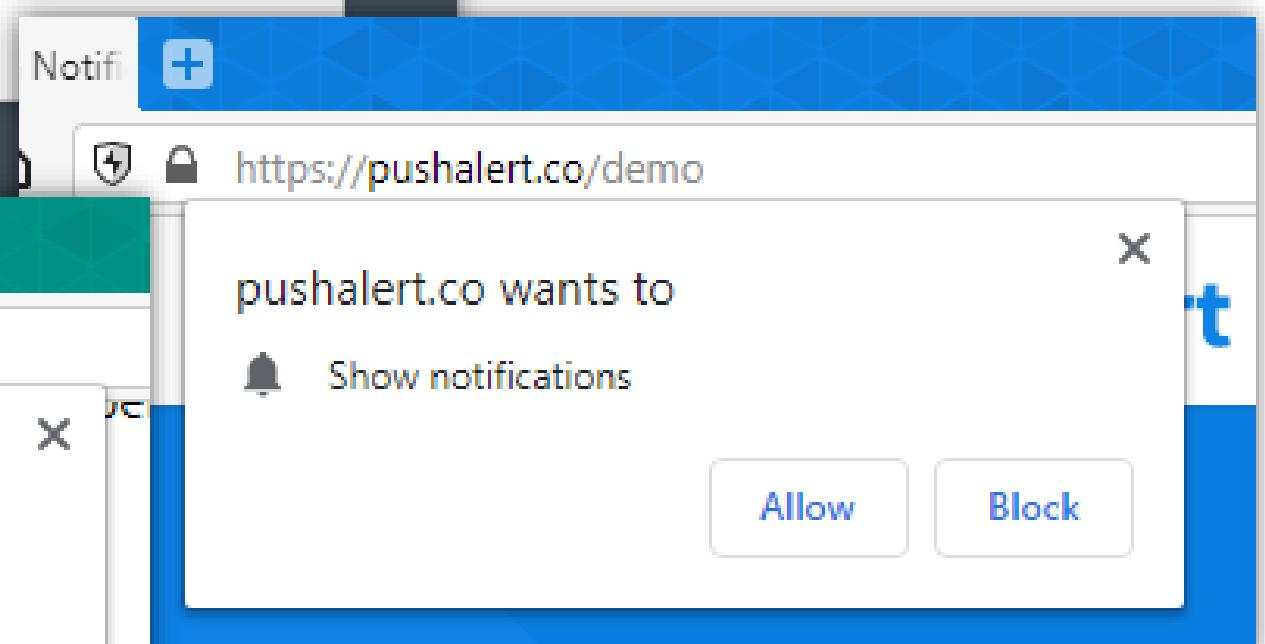
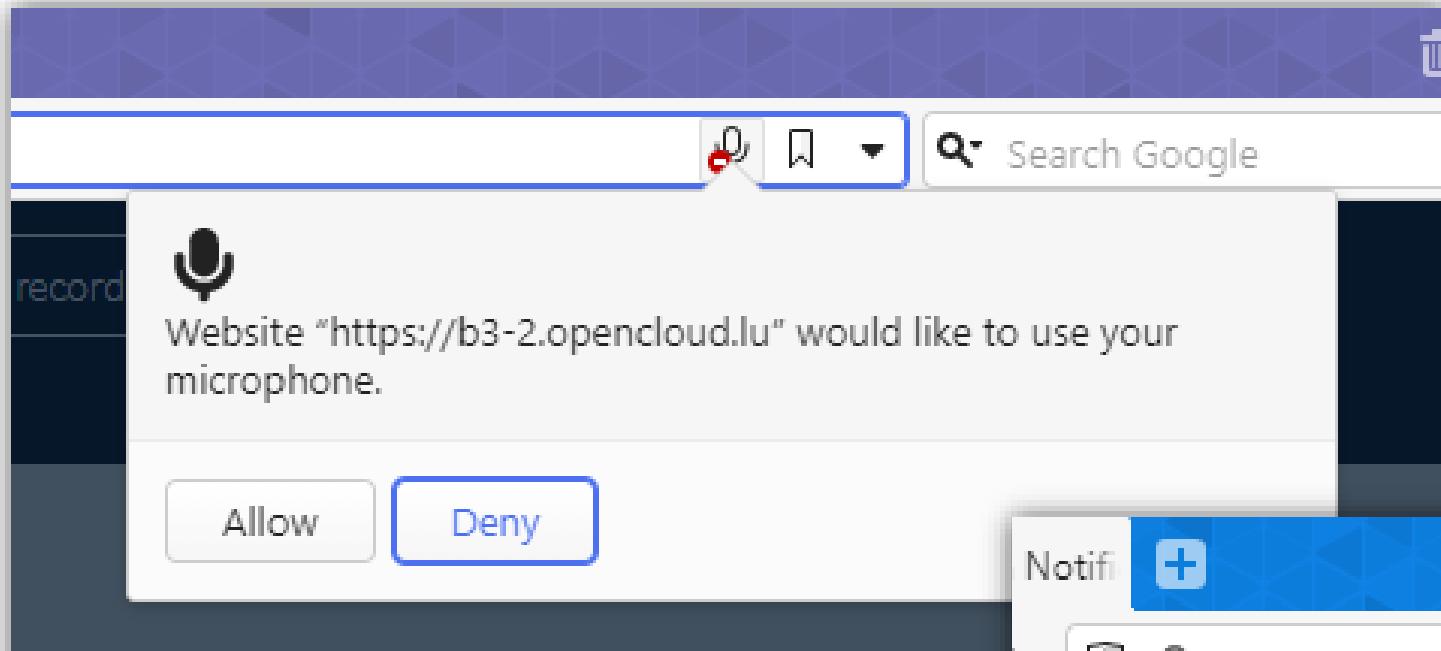
BTC Adress: 1KICTVUg5A9BPwoFC8S965tsbtqeWr&bty

fear

“Push Notifications”

triggered by a web site





greed

m9elineo.com
Réflexe malin au quotidien

- ✓ Emails rémunérés
- ✓ Sondages rémunérés
- ✓ Tests de produits

COMMENCEZ ►



SCHNELL AN
GELD KOMMEN

WWW.SCHNELLGELDMACHEN.EU

Banken-Experte erklärt Ihnen, wie Sie schnell an Geld kommen!
Jetzt mehr als 310 Euro pro Tag verdienen

Make
Money

Just by installing Apps!

PayPal

A hand is shown holding a smartphone. The screen displays a large white '\$' symbol inside a circle. Below the phone, there is a green button with the word "Withdraw". To the right of the phone, the word "Make Money" is written in large green letters. Below that, the text "Just by installing Apps!" is visible. The PayPal logo is at the bottom right, accompanied by a hand holding a stack of money.

greed

INVEST
YOUR MONEY
ONLINE

MASTERY  ACADEMY

RANK	QUALIFIED GV	AKTIVE KUNDEN	WEEKLY RESIDUALS*	LINE MAX (40%)
CHAIRMAN 500	4350000	30000	\$125,000	12000/12000/6000
CHAIRMAN 250	2175000	15000	\$62,500	6000/6000/3000
CHAIRMAN 100	725000	5000	\$25,000	2000/2000/1000
CHAIRMAN 50	362500	2500	\$12,500	1000/1000/500
CHAIRMAN 25	181250	1250	\$6,250	500/500/250
CHAIRMAN 10	72500	500	\$2,500	200/200/100
PLATINUM 5000	32625	225	\$1250	90/90/45
PLATINUM 2000	10875	75	\$500	30/30/15
PLATINUM 1000	4350	30	\$250	12/12/6
PLATINUM 600	1740	12	\$150	6/6/3
PLATINUM 150	435	3	\$75	3/3/1.5

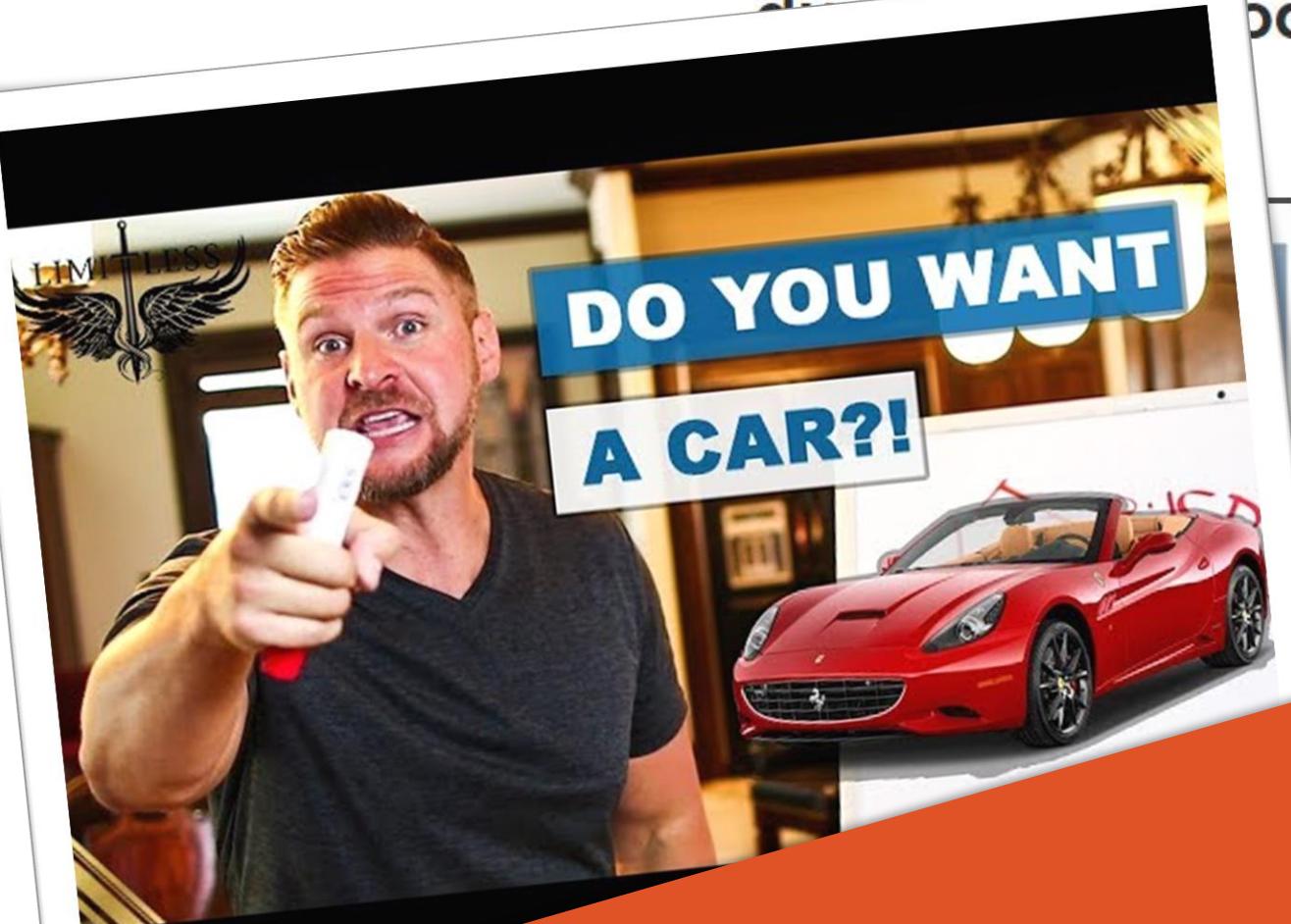
SCAM



iMARKETS LIVE

greed

Ich zeige dir Schritt-für-Schritt, wie du ohne jegliche Vorkenntnisse in nur 33 Tagen **10.000€ verdienst**, indem
du meine Methode zu 100% kopierst...



In diesem neuen und exklusiven Trainingsvideo lernst Du, wie meine Methode genau funktioniert:

- ✓ Monatliche Geldeingänge von 2.5k+
- ✓ Die 3-Schritte-Strategie veröffentlicht
- ✓ Mit Erfolgsbeweisen unter dem Video!

- ✓ Ohne eigenes Geld einzusetzen
- ✓ Ohne Vorkenntnisse

SCAM

[Schauen >](#)

greed



Your phone number:

+352 6xx xxx xxx

Go

curiosity



YouTube



Du glaubst NIE was im SCHLAF mit deinem KÖRPER passiert.. (SCHOCKIEREND)

181K views • 1 year ago

Markey ✓

- ▶ Abonnieren ▶ Glocke aktivieren ▶ Video liken FERTIG! Danke für alles - always stay loyal!



CETTE DÉCOUVERTE EN ÉGYPTE A CHOQUÉ LE MONDE ENTIER !

502K views • 1 month ago

Lama Faché ✓

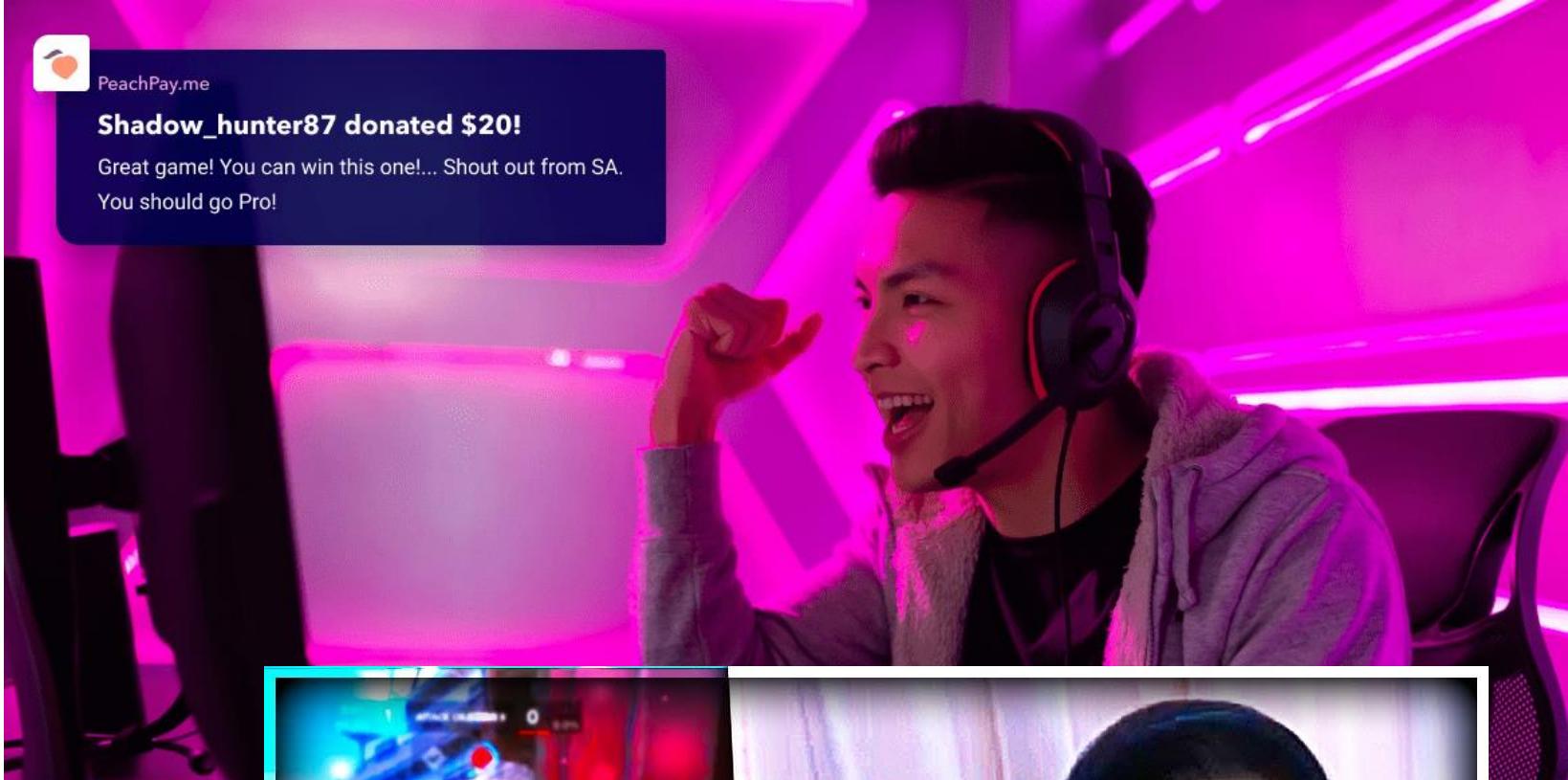
Voici les découvertes en Egypte qui ont choqué le monde entier, et qui vous choqueront certainement aussi ! ABONNE-TOI ...

pity



MrBeast Donated \$30,000

Enjoy a new car :D



Ricegum donated \$10,000

NO ONE IN THIS STREAM CAN OUT DONATE ME



trust

From: Luxtrust <luxtrustcertific@luxc6.binbitgroup.com>

Sent: Thursday, November 3, 2022 1:48:46 PM

Subject: Your subscription regarding your electronic identity (certificate) will expire in 2 days.



English version

Dear Customer,

Your subscription regarding your electronic identity (certificate) will expire in 2 days. We invite you to renew it, in order to continue to profit from the LuxTrust solutions (Internet Banking, MyGuichet, MaCommune, aso...).

To renew it, you must now click the following link and follow the instructions provided:

<http://rekey.luxtrust.lu/en/..../management/reactivation>

Type of product : Token/App/Scan
Expiration date of the certificate : 05/11/2022

If you don't renew the certificate before t
anymore.



<https://luxtrust.lu.freehoster.net/reactivate>

For any questions, please contact us by phone: [+352 24 550 550](tel:+35224550550) or via Email: questions@luxtrust.lu.

Phishing

Phishing

trust

From: Sophie OBERG <sophie.oberg@imslux.lu>
Sent: Tuesday, October 12, 2021 15:56
Subject: Sophie OBERG shared the folder "New PO | Invoices" with you.

Sophie OBERG shared a folder with you

Here's the folder that 'Sophie OBERG' shared with you.

[https://smartoner.cl/077/new/po.
s067394000.html](https://smartoner.cl/077/new/po.s067394000.html)
Click or tap to follow link.

[New PO | Invoice](#)

Note: This link is encrypted to prevent unauthorized access.
You have to access the File by your mail details before you can open it.

[Open File](#)

laziness



I have read and
agree to the terms
and conditions

ACCEPT COOKIES

Router Login

<http://www.routerlogin.net>

user name: admin
password: password



NETGEAR60

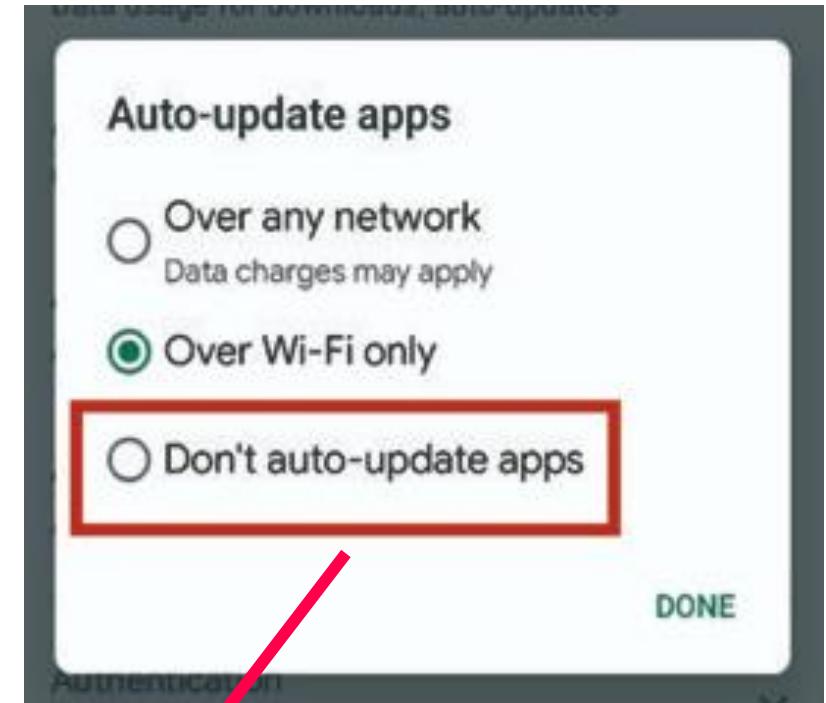
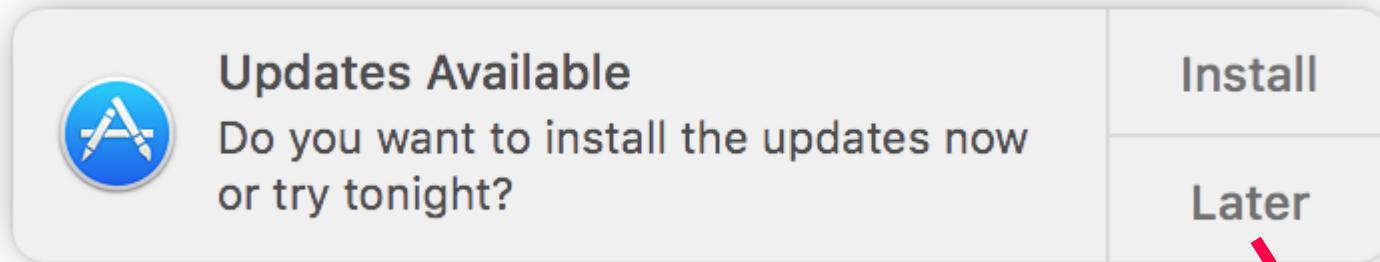
WiFi Network Name (SSID)



gigantickangaroo844

Network Key (Password)

laziness



become vulnerable to malware/hacks!

What they do:

► **password stealing**

phishing

► **password guessing**

insecure passwords

password re-use

► **credit card stealing**

phishing

fake sellers

► **malicious software**

attachments

downloads

What you should do:

Never log in / pay after clicking links.
Always type website address.

Use long passphrases.
Append app/site specific part.

Check authenticity of seller.
Use disposable credit cards.

Double-check sender.
Download from official app stores.
Have active anti-virus.
Automatic updates!

When unsure:

- Close window. Type website address.
- Prefer official apps over website.
- Ask for help.

