

# **>MALICIOUS CONTENT**



# Malicious Content

<https://Malicious-Content.com>

## The Rules

- Each player draws 2<sup>3</sup> red cards. The player with the most recent security incident begins as the blue team, turns over and reads aloud a blue card. Everyone else (the red team) plays one or more red cards face down to fill in the blank(s).
- The blue team shuffles and reads aloud each combo, picking the winning red card. Whoever played the answer keeps the blue card for scoring.
- The blue team role shifts to the left for the next round, and everyone draws back up to 10 red cards.
- *Hack the rules to your liking, push to prod!*

## The Creds

This work is licensed by Jon Camfield under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. Thanks to everyone who's shared card ideas or whiskeys along the way. Lock icon by Font Awesome, PFTempesta font by Yusuke Kamiyamane and there's probably some jquery in here too.



»MALICIOUS CONTENT\_

**>MALICIOUS  
CONTENT**



# The Magister Pecuarius

"The Magister Pecuarius:  
The Analyst should not  
dismiss the reasonable  
potential of an attacker  
using trained animals to  
circumvent barriers and  
obstacles where a  
human being cannot."

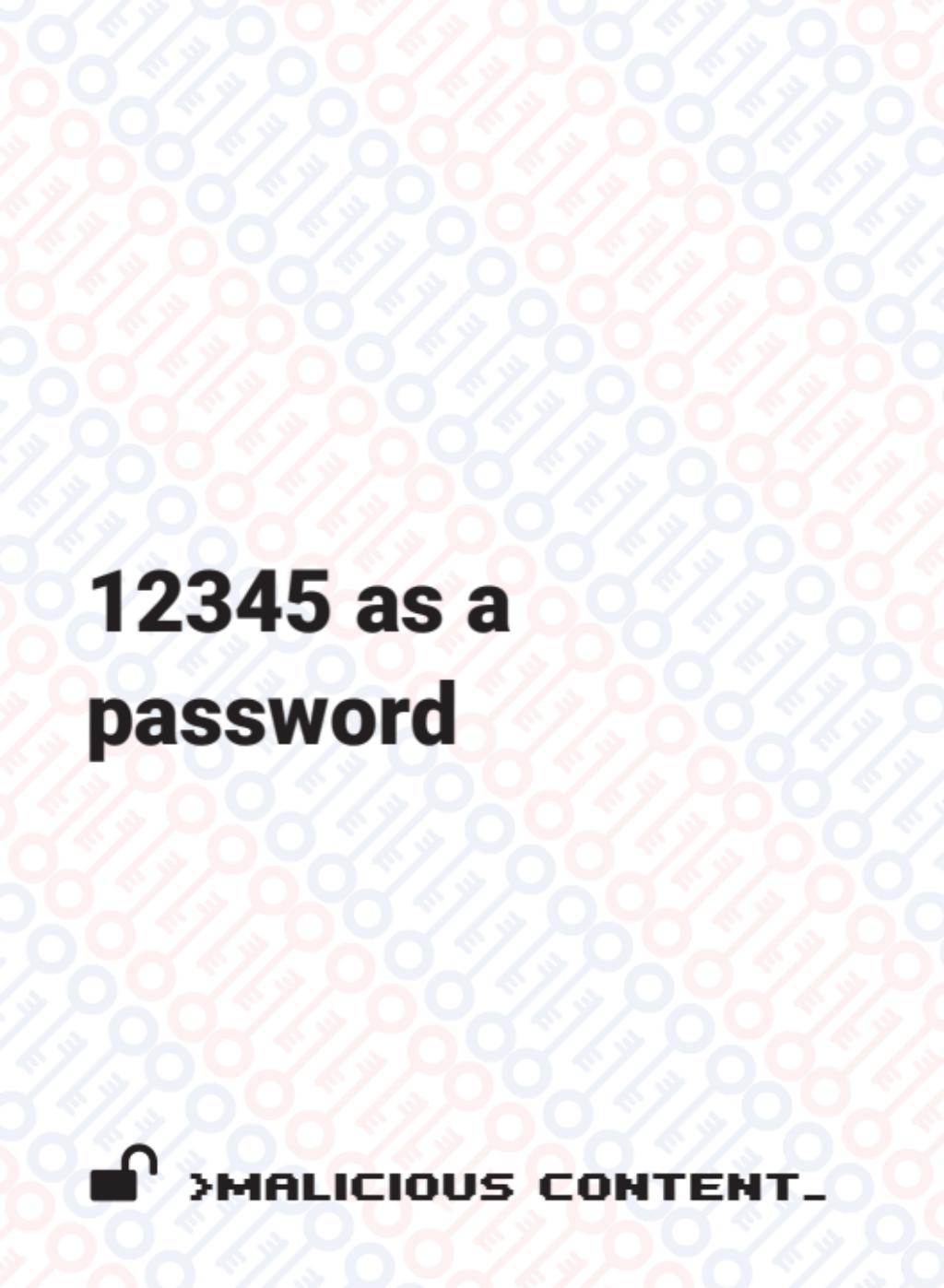
OSSTMM3



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





# **12345 as a password**



**→MALICIOUS CONTENT→**

**>MALICIOUS  
CONTENT**



# **admin accounts for everyone**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **Advanced Persistent Threats**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



# **attribution dice**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **"Big Data" with small data sets**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **Bitcoin**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





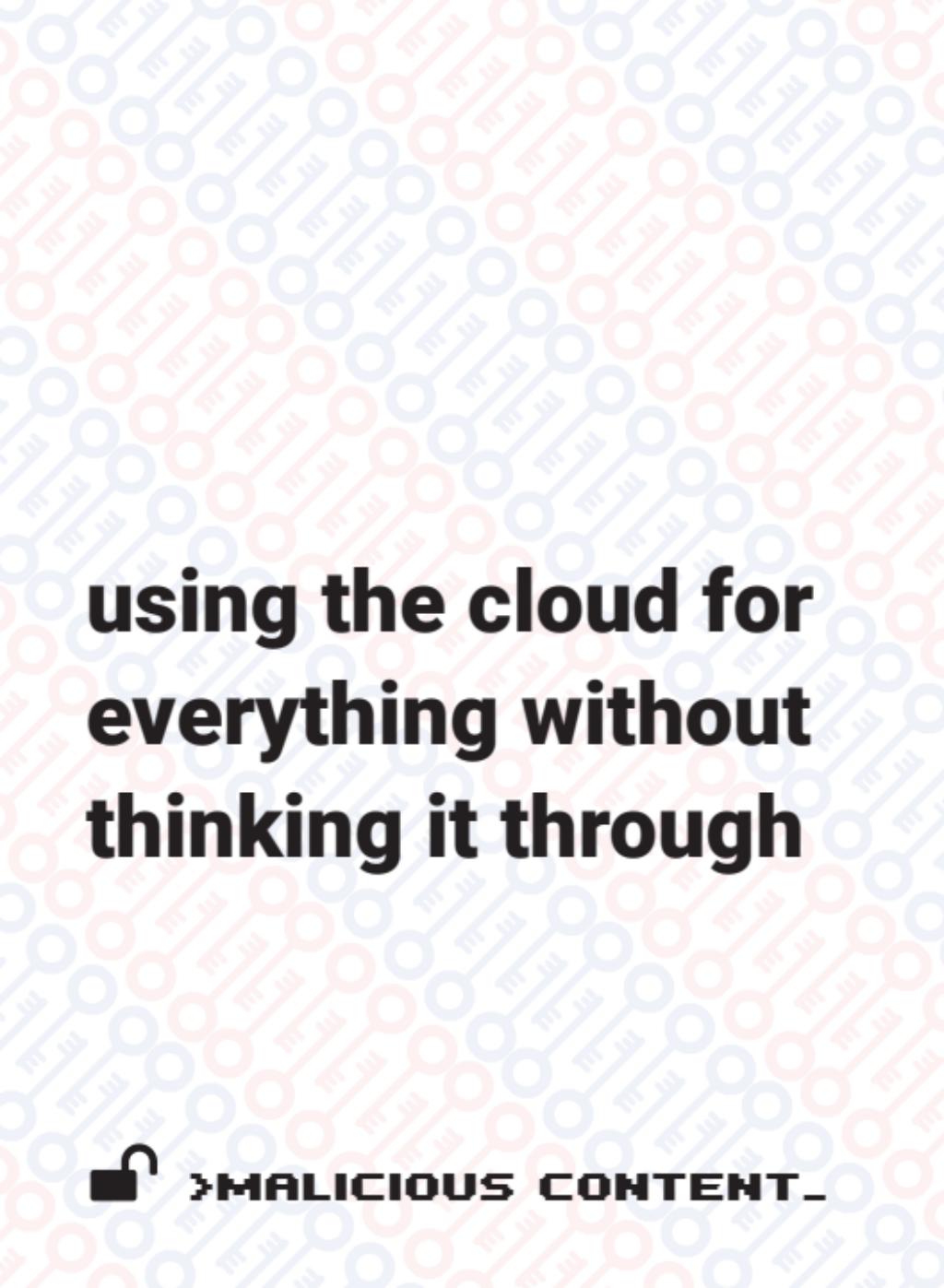
# **the (motherfuckin') blockchain**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





**using the cloud for  
everything without  
thinking it through**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





# **private conversations in co- working spaces**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





# "cyber"



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**



# **DEFCON attendees**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





# **weaponized, wifi- enabled drones**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





# **distributed denial of service attacks**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# hackathons



**→MALICIOUS CONTENT→**

**>MALICIOUS  
CONTENT**





# **developer-centered design**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **Linux on the desktop**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **mailing lists and wikis**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **mansplaining**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





# **netflix and chill**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **PGP for the average user**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





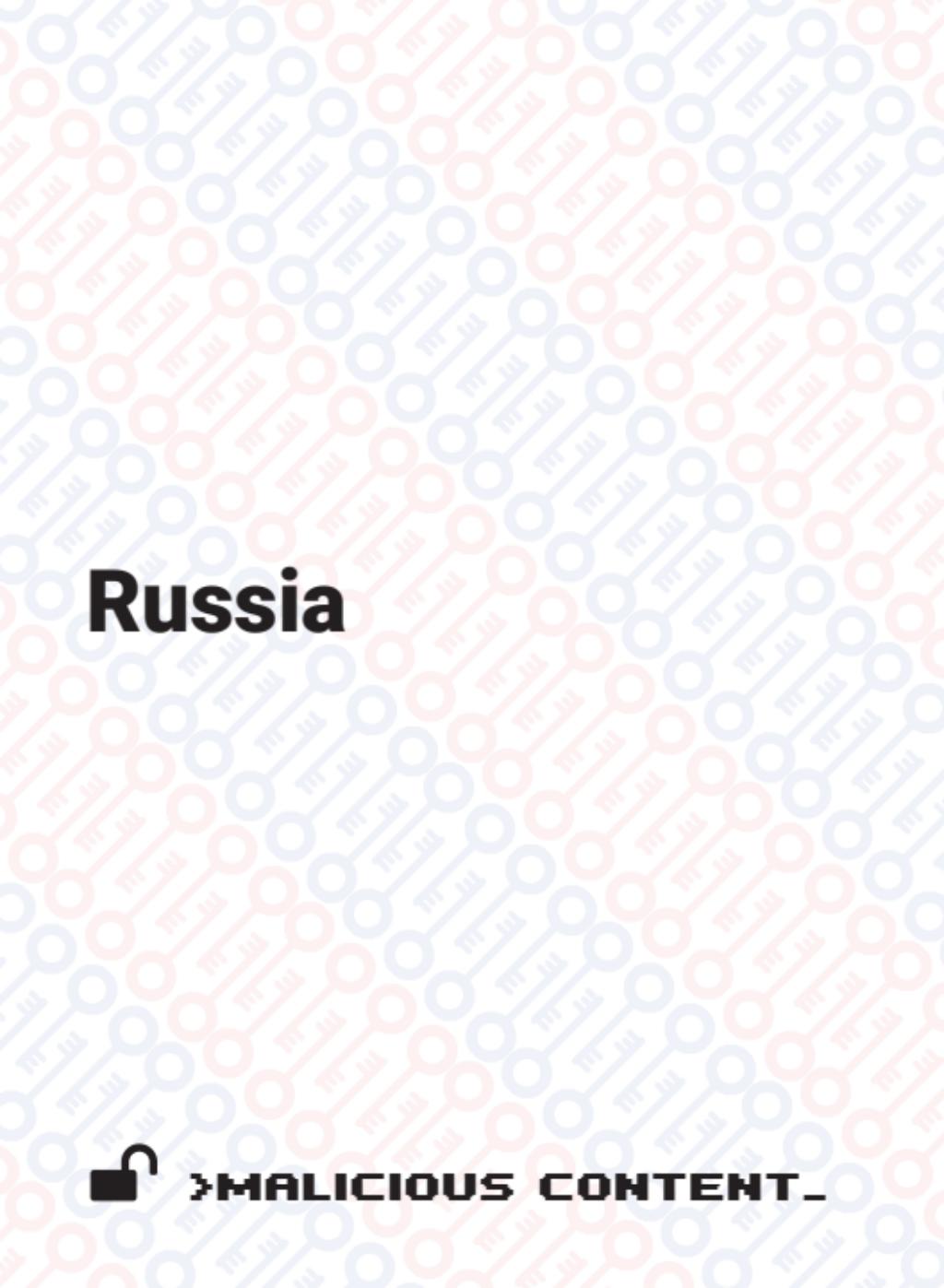
**porn**



**>MALICIOUS CONTENT.**

**>MALICIOUS  
CONTENT**





# Russia



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



# **Skype calls to discuss communication security**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





# **detail-free threat information sharing**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





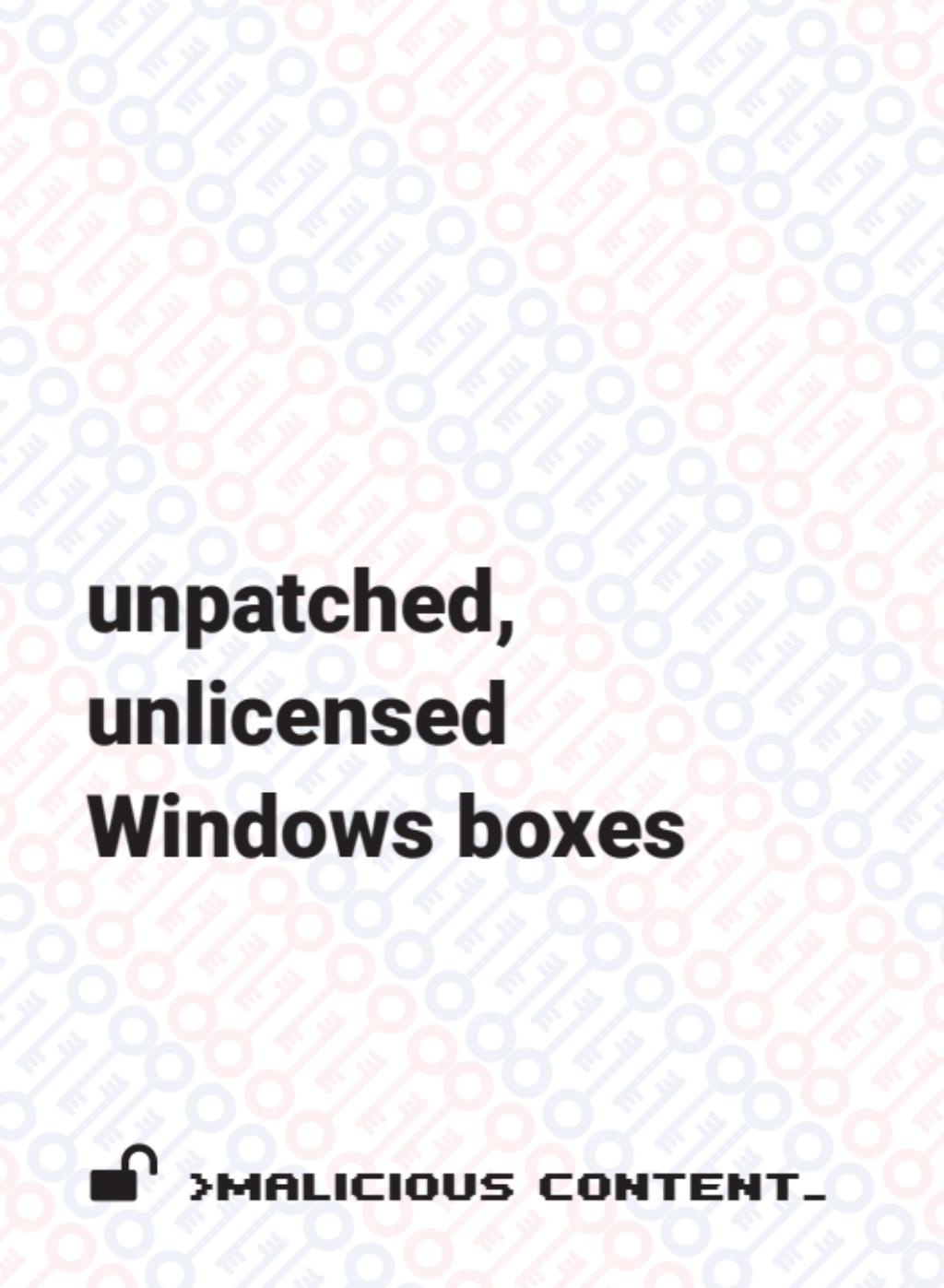
# trolling



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





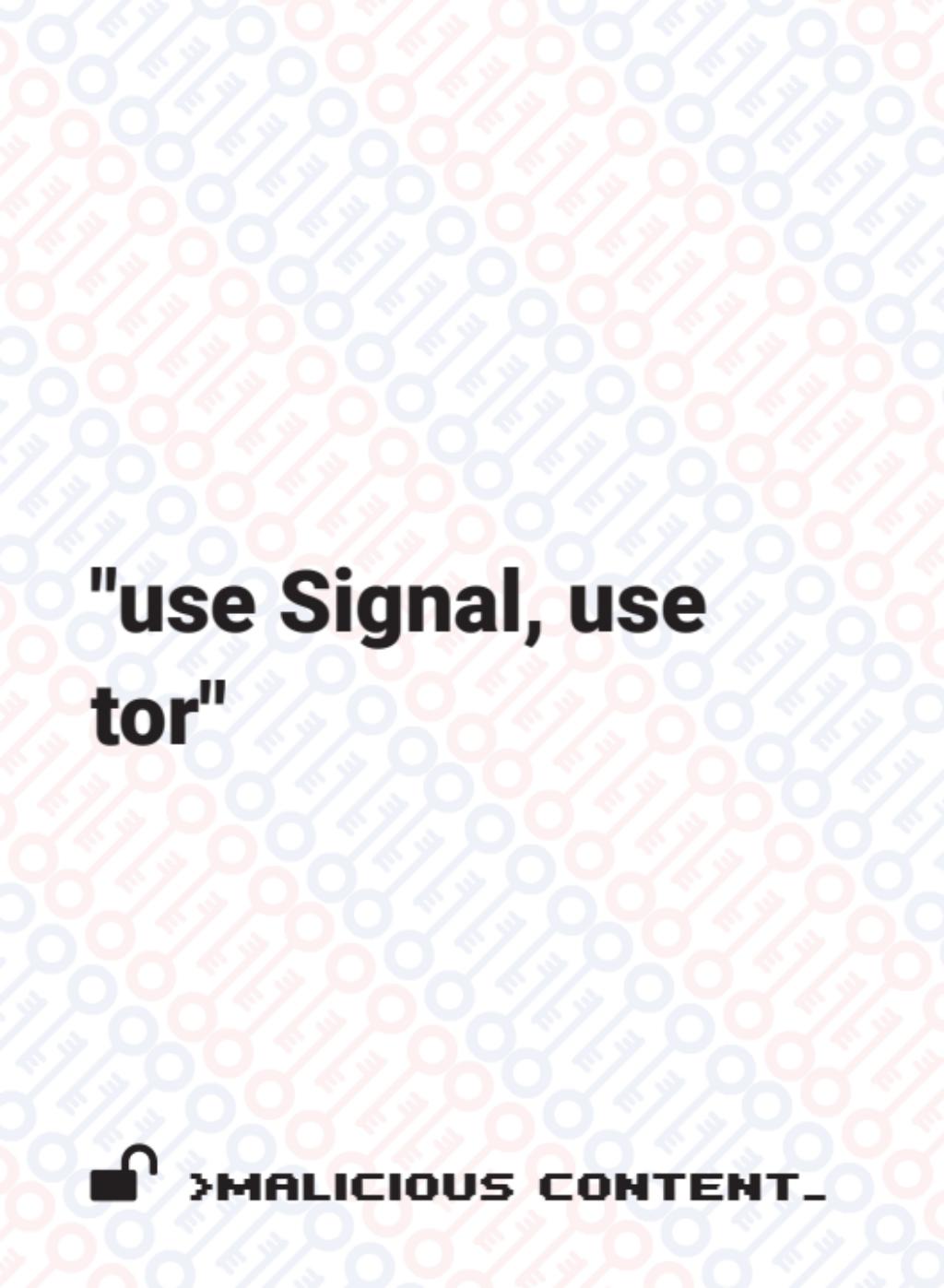
# **unpatched, unlicensed Windows boxes**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





# **"use Signal, use tor"**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# troll farms



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**



# **RFC 2549 compliant encrypted carrier- pigeons**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# Fancy Bear



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





**correct horse  
battery staple  
(xkcd.com/936)**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **Flash as a hard requirement**



**>MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **the 'dark web'**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**



# **rolling your own crypto**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





# **the undying hopelessness of our profession**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**



# 1 Factor Authentication



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



# onion dildonics



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **tor exit nodes**



**→MALICIOUS CONTENT→**

**>MALICIOUS  
CONTENT**



# Club Mate



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **the good whiskey**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





**stock photos of  
hooded hackers lit  
by the glow of a  
screen**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





# **overly confident spokespeople**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **tinfoil hats**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





# **offshore data havens in dubious jurisdictions**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# Rubber-hose cryptoanalysis



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





# **Project Zero's issue queue**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **getting @'d by taviso on Friday**



**>MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



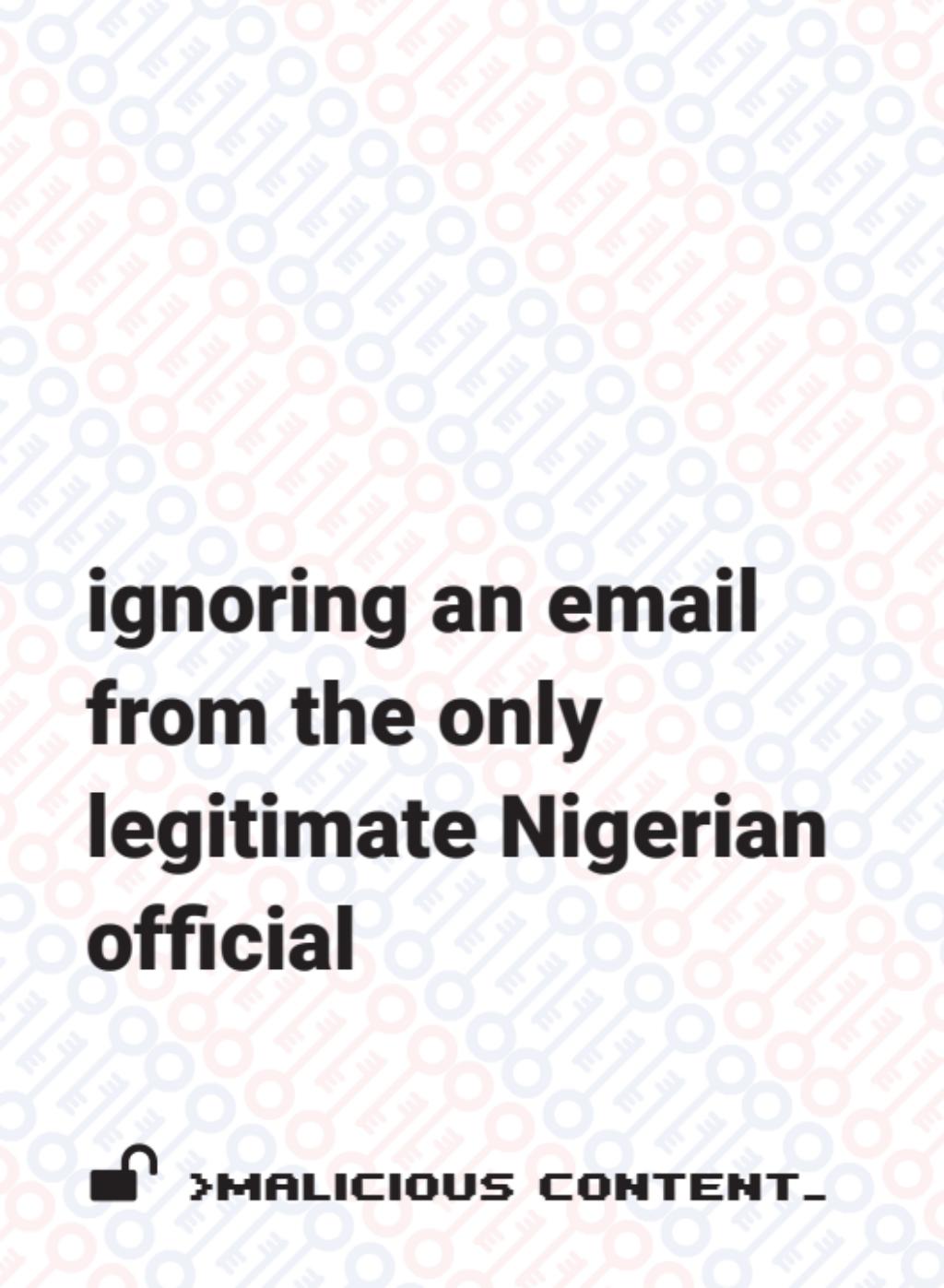
# **sexting**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





**ignoring an email  
from the only  
legitimate Nigerian  
official**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





# **smart devices with dumb passwords**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





# **finding out IT bought FinFisher for remote administration**



**»MALICIOUS CONTENT«**

**>MALICIOUS  
CONTENT**





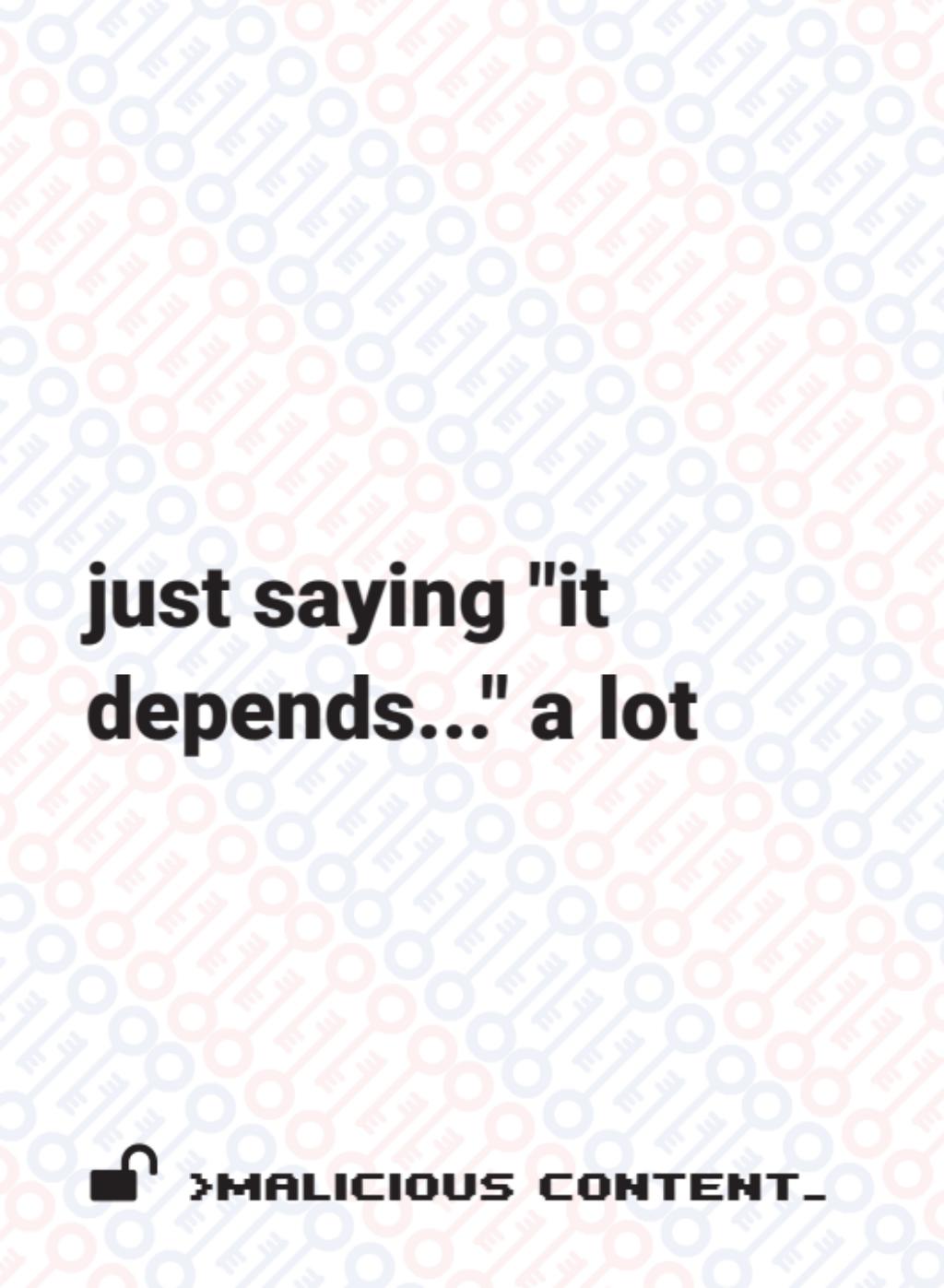
# **infosec shitposting on twitter**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





**just saying "it  
depends..." a lot**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





# **"Internet of things" botnets**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **127.0.0.1 as an indicator of compromise**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





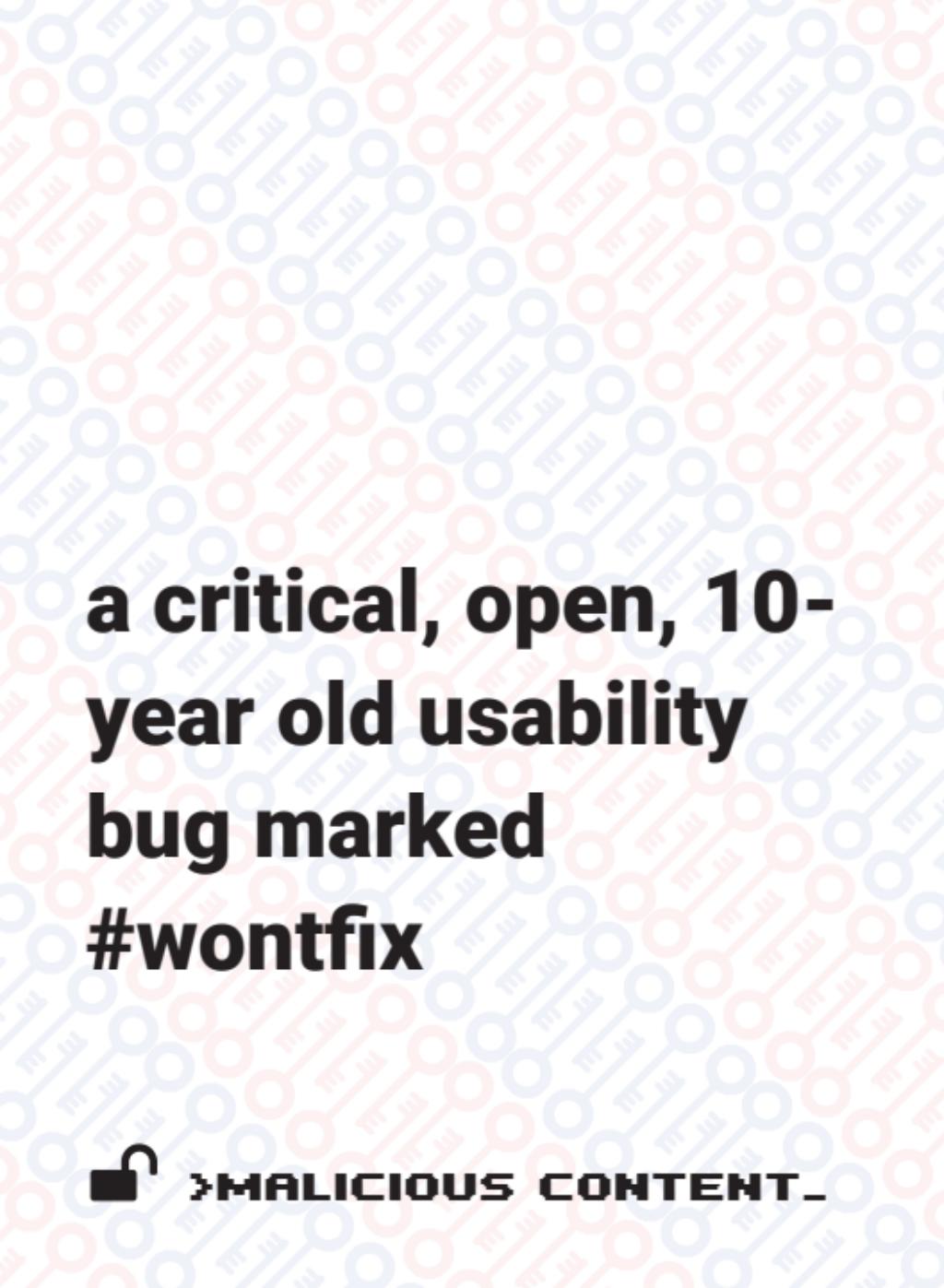
# **hotel 'staff'**



**>MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





**a critical, open, 10-  
year old usability  
bug marked  
#wontfix**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**





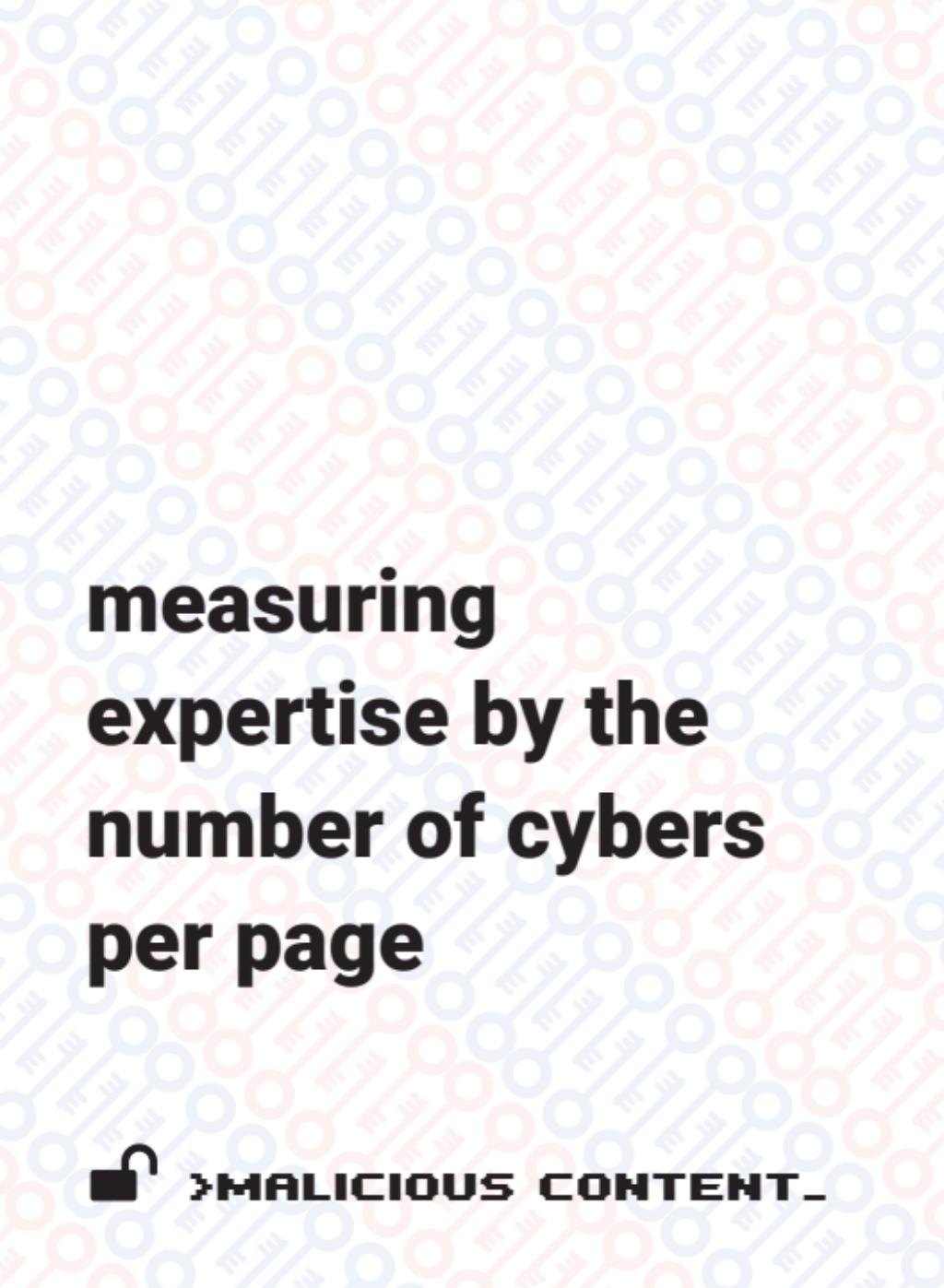
**entry/exit policies  
that don't cover  
social media  
accounts**



**→MALICIOUS CONTENT→**

**>MALICIOUS  
CONTENT**





**measuring  
expertise by the  
number of cybers  
per page**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **hacking back**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



# The NSA



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



# Facebook



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



# **app stores**



**→MALICIOUS CONTENT→**

**>MALICIOUS  
CONTENT**



# squirrels



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



# **network neutrality**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**





**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**





**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **meetings at Casey's Coffee**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **internet freedom grant proposals**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **fragile states**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **cyber-unfree countries**



**>MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

**rejecting  
government  
funding in favor of  
corporate funding**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **1-page copypasta risk assessments**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **vulnerable populations**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **freedom of expression**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **diaspora communities**



**>MALICIOUS CONTENT-**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **Internet shutdowns**



**MALICIOUS CONTENT**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

**yet another digital  
security training/  
guide/curricula**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **The eternal confusion between a guide and a curricula**



**»MALICIOUS CONTENT\_**

**>MALICIOUS  
CONTENT**



**INTERNET FREEDOM BONUS PACK**

# **Glitter**



**>MALICIOUS CONTENT-**

**»MALICIOUS  
CONTENT\_**



# A blockchain for

---



**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





# **Artisanal, handcrafted malware to target**

---



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





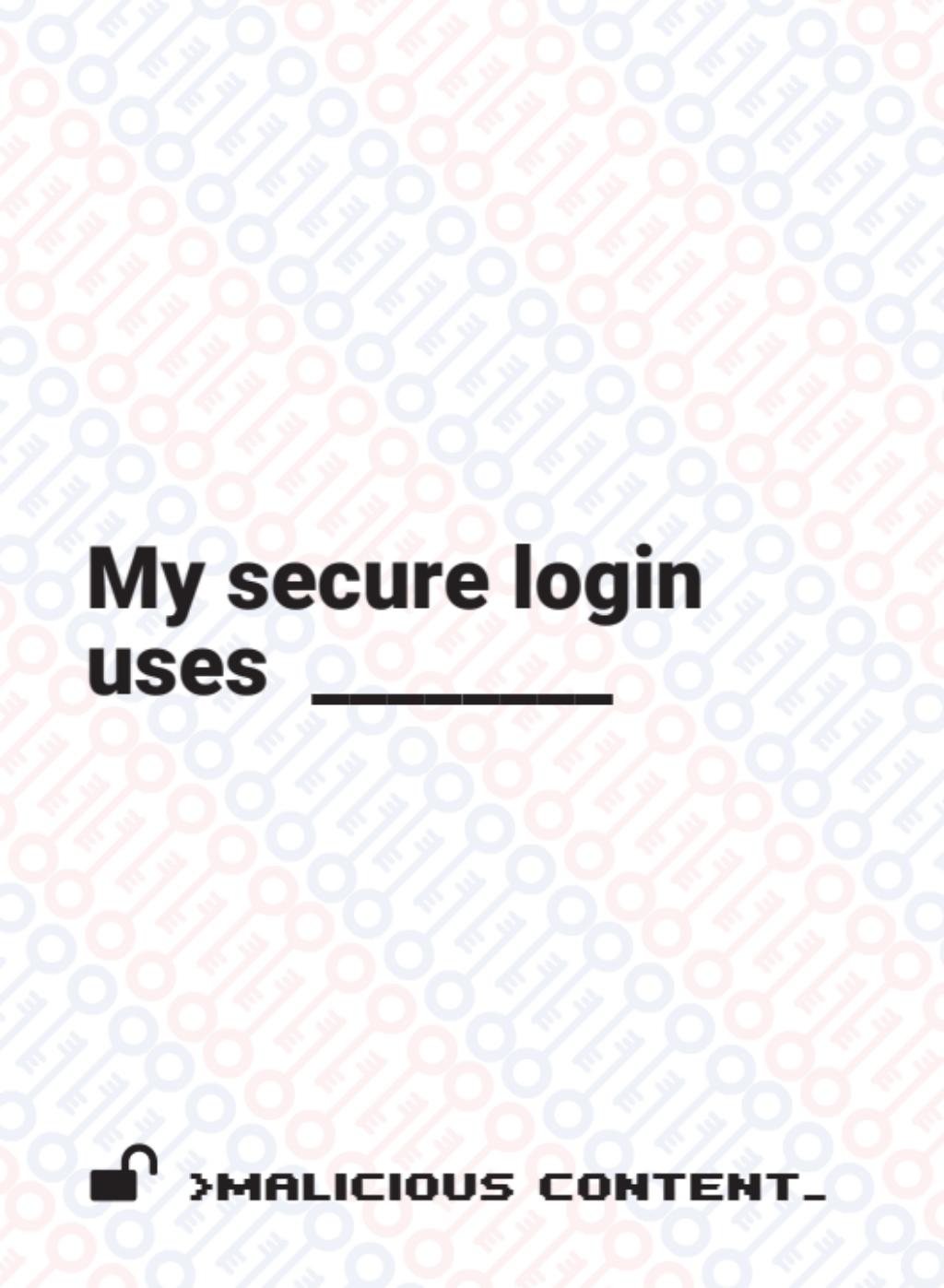
# Cyber-\_\_\_\_\_



**►MALICIOUS CONTENT.**

**»MALICIOUS  
CONTENT\_**





# **My secure login uses \_\_\_\_\_**

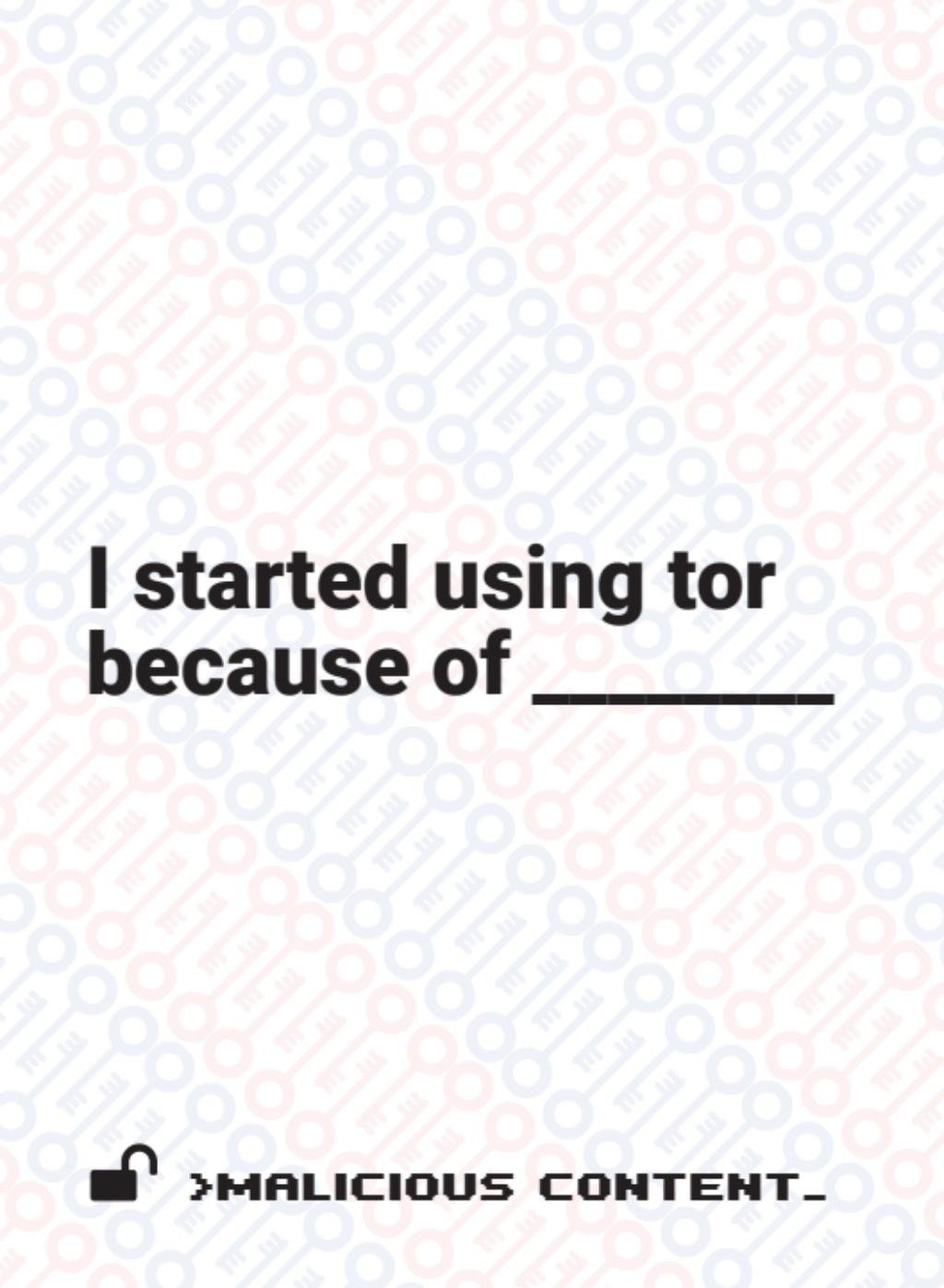
---



**►MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





**I started using tor  
because of \_\_\_\_\_**



**»MALICIOUS CONTENT.**

**»MALICIOUS  
CONTENT\_**





**We're launching a  
next-generation  
anti-virus solution  
for \_\_\_\_\_**



**►MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



# I explain PGP using

---



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**



---

# **over secure messaging**



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**



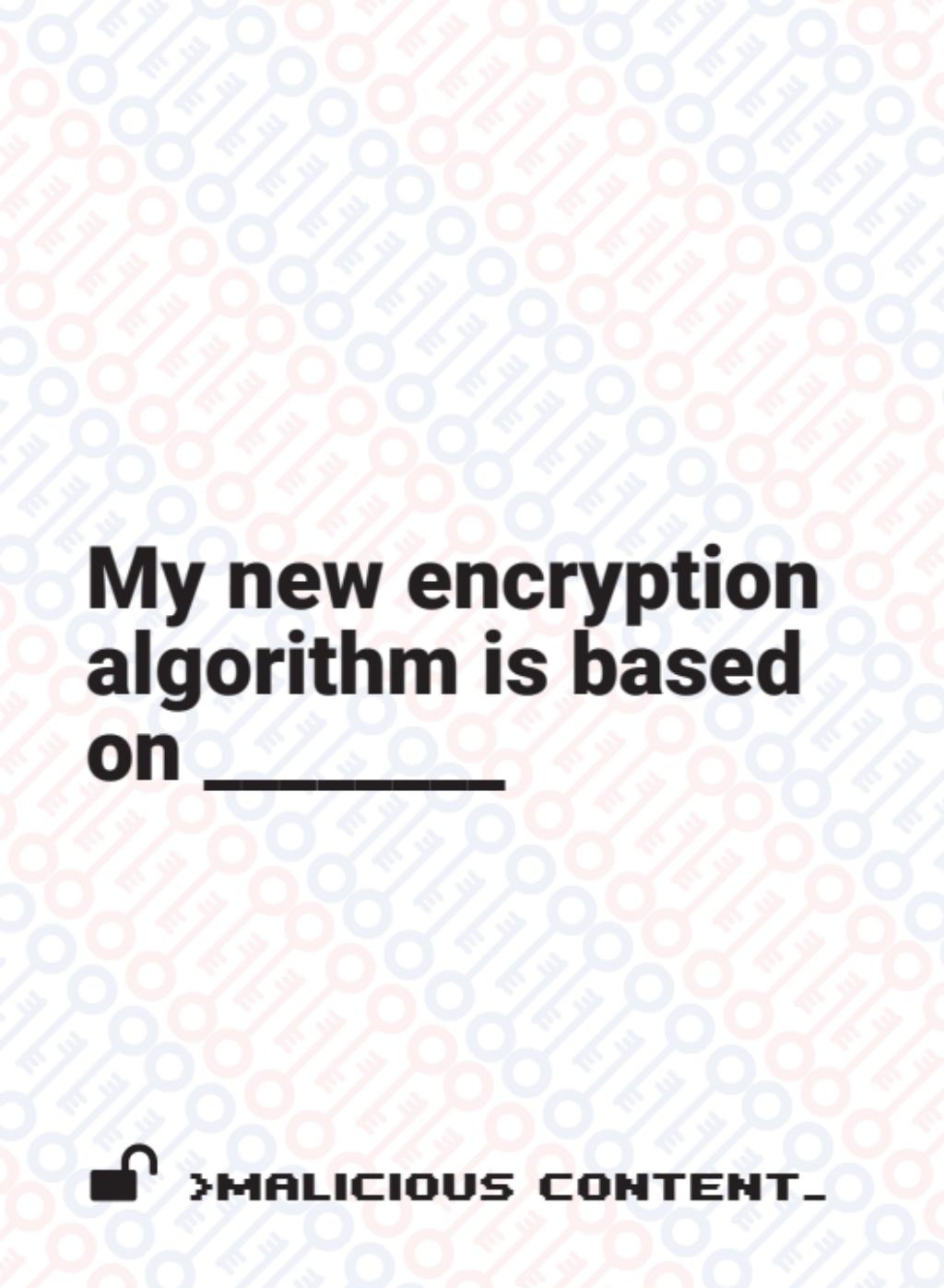
**It's like \_\_\_\_\_ but  
for \_\_\_\_\_**



**➤MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





**My new encryption  
algorithm is based  
on \_\_\_\_\_**



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





**Malware is now  
being distributed  
through \_\_\_\_\_**



**►MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





**Dual-use  
surveillance  
technology exports  
are being  
legitimized by**

---



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





# **Threat information sharing for the \_\_\_\_\_ community**

---



**»MALICIOUS CONTENT»**

**»MALICIOUS  
CONTENT\_**



# **The silver bullet solution for \_\_\_\_\_ is \_\_\_\_\_**



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





**The next Russian  
APT group will be  
named \_\_\_\_\_  
Bear**



**►MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



I turned to \_\_\_\_\_  
after the \_\_\_\_\_  
0day



►MALICIOUS CONTENT-

**»MALICIOUS  
CONTENT\_**





**Last week's hack  
mostly impacted  
the \_\_\_\_\_  
community.**



**►MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



# **Military Grade**

---



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





# **Confidentiality, integrity and**

---



**»MALICIOUS CONTENT\_**

**»MALICIOUS  
CONTENT\_**



---

# **over tor**



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**



# Pretty Good

---



**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





# **My threat model is based entirely on**

---



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





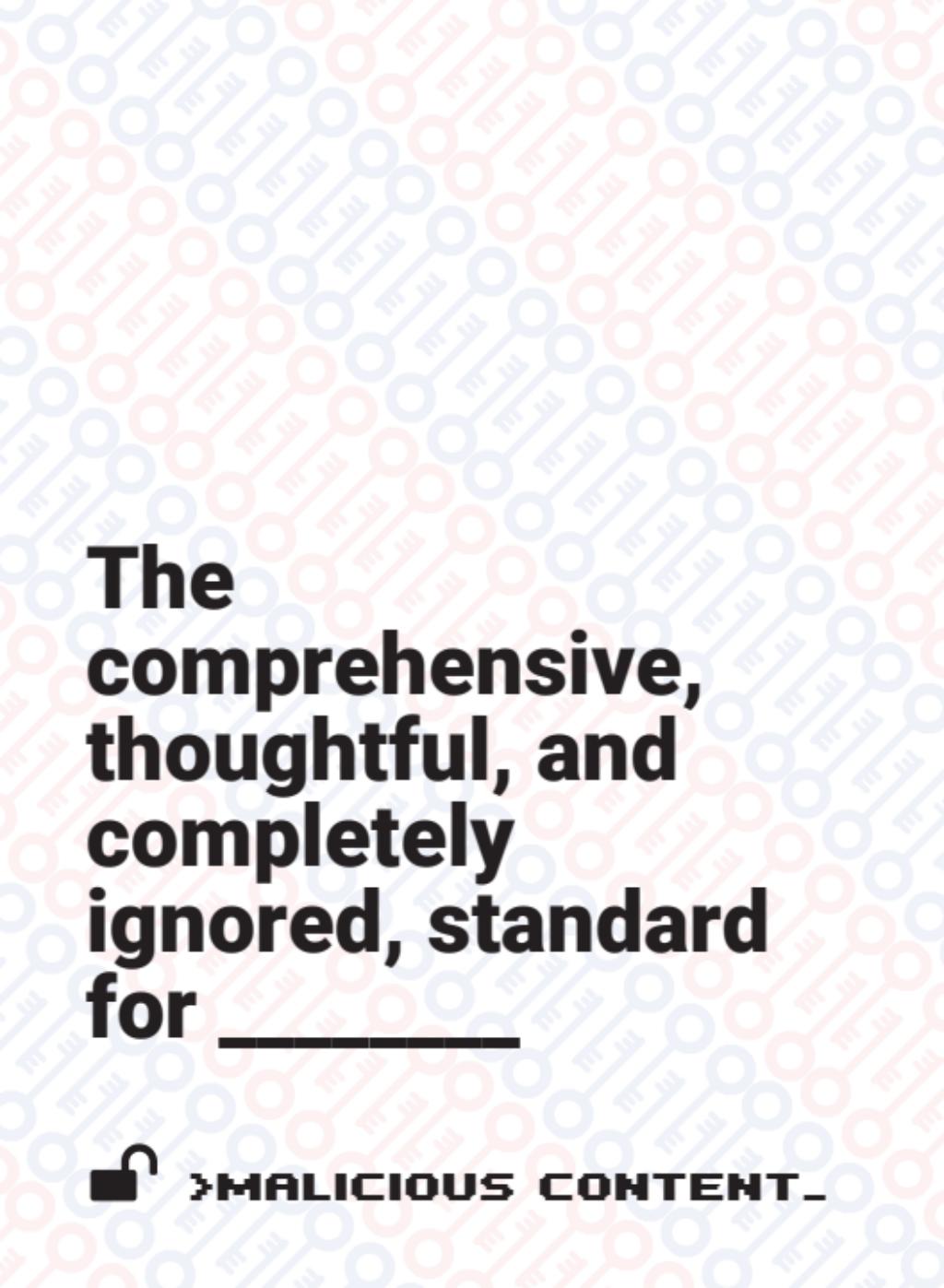
**I don't consider \_\_  
as part of my threat  
model**



**→MALICIOUS CONTENT→**

**»MALICIOUS  
CONTENT\_**





**The  
comprehensive,  
thoughtful, and  
completely  
ignored, standard  
for \_\_\_\_\_**



**►MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



---

# **in the middle**



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





**The pentester  
succeeded, thanks  
to \_\_\_\_\_**



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**



# The next branded vulnerability will break \_\_\_\_\_



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**





**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



**INTERNET FREEDOM BONUS PACK**

**USG funded**

---



**>MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



**INTERNET FREEDOM BONUS PACK**

# **A venture capital styled approach for**

---



**»MALICIOUS CONTENT«**

**»MALICIOUS  
CONTENT\_**



**INTERNET FREEDOM BONUS PACK**

# **Mesh-enabled**

---



**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**



## INTERNET FREEDOM BONUS PACK

**According to  
Freedom on the  
Net, this is the 7th  
consecutive year of  
decreasing**

---



**MALICIOUS CONTENT**

**»MALICIOUS  
CONTENT\_**





**My digital security  
trainings now only  
cover \_\_\_\_\_**



**»MALICIOUS CONTENT«**