Security Solutions


Password:
Pick good passwords. Never use the default.

EPISODES - SEASON 46

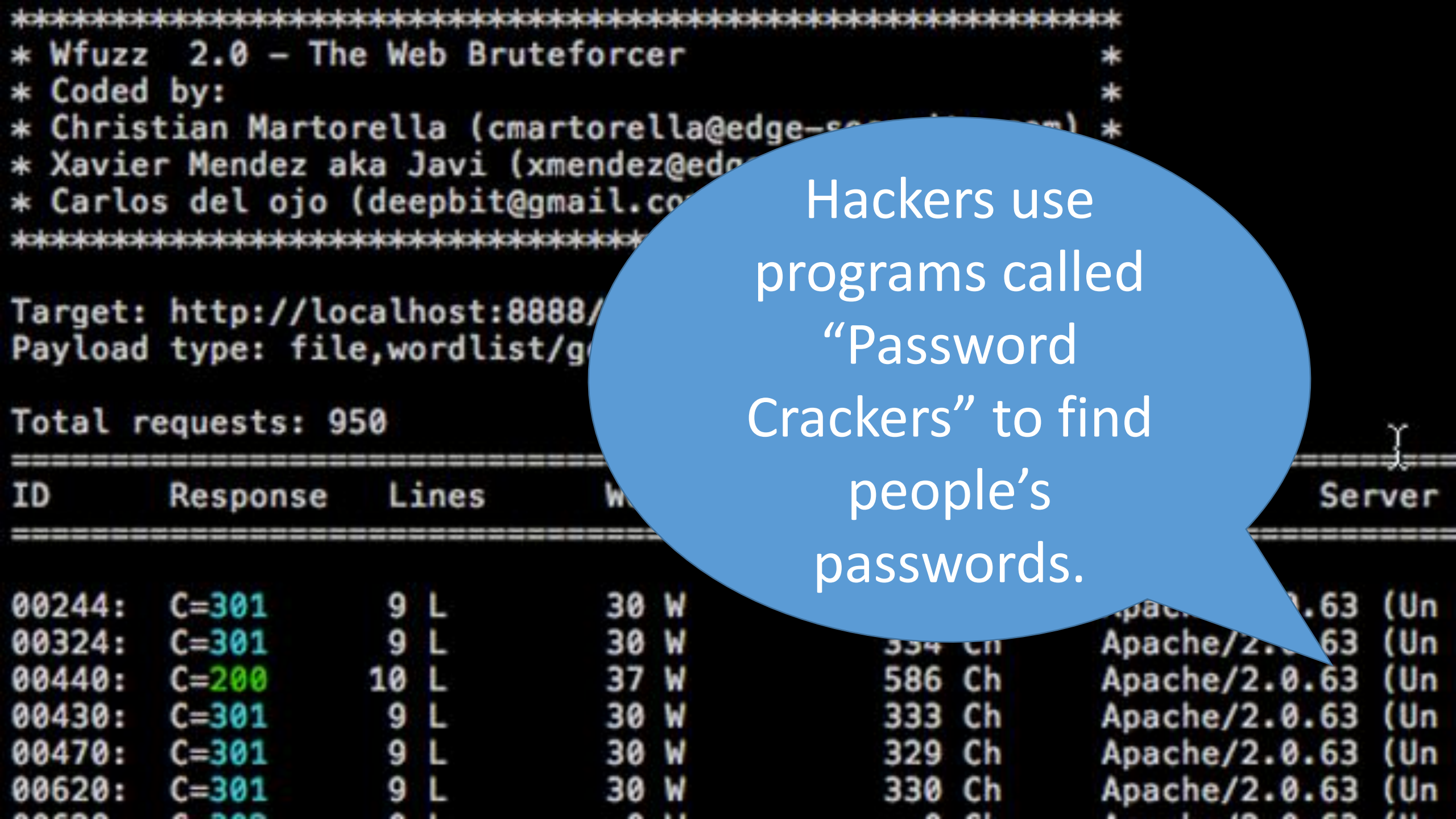
@cbcmarketplace

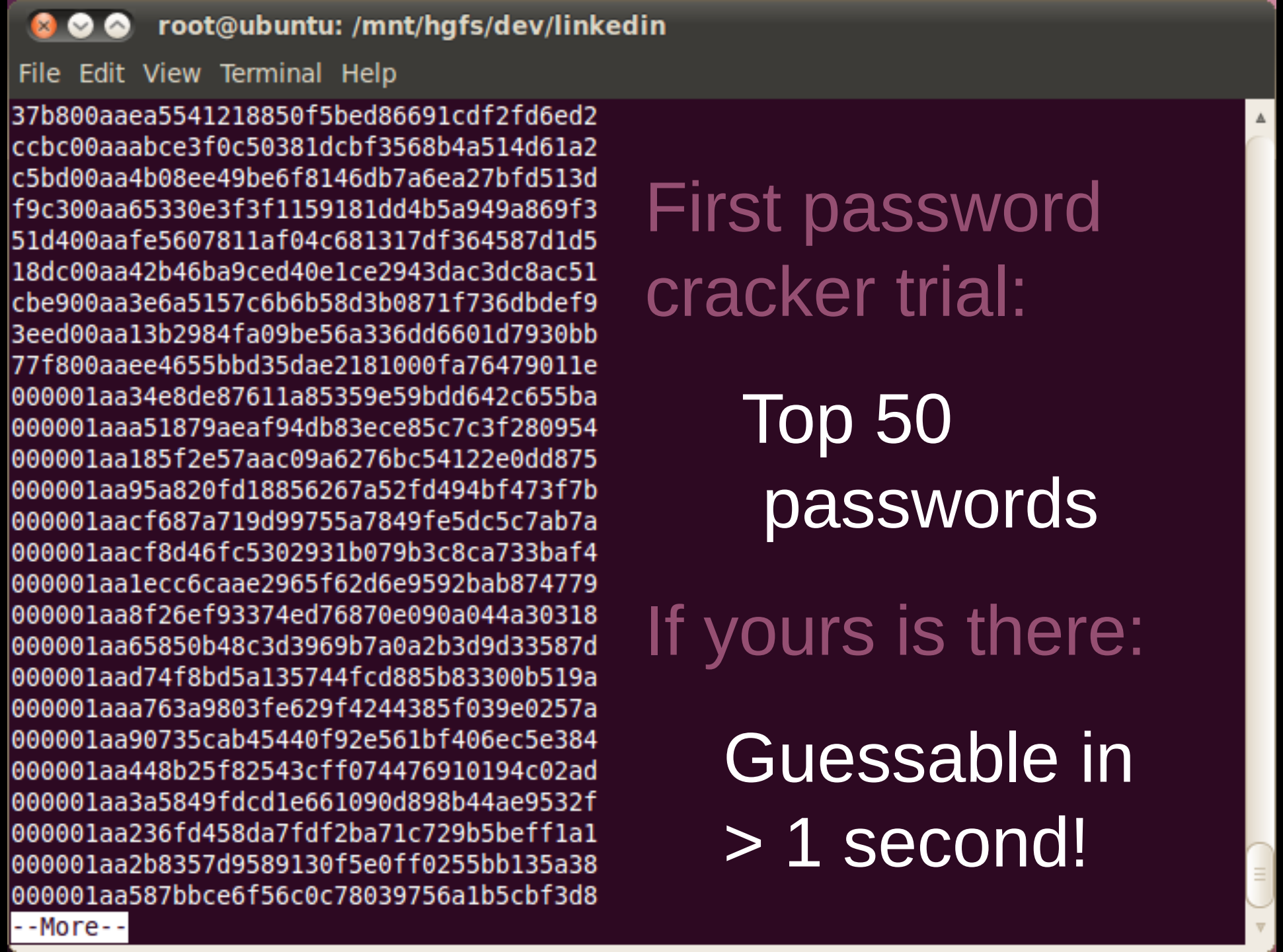
BROADCAST DATE : SEP 28, 2018

Home Hack: How safe are your high-tech security devices?

Remember the Alexa hack?

They got in through weak passwords – one person used the default…


* Wfuzz 2.0 - The Web Bruteforcer *
* Coded by: *
* Christian Martorella (cmartorella@edge-
* Xavier Mendez aka Javi (xmendez@ed
* Carlos del ojo (deepbit@gmail.co
Target: http://localhost:8888/
Payload type: file,wordlist/g
Total requests: 950
ID Response Lines W Server
00244: C=301 9 L 30 W .63 (Un
00324: C=301 9 L 30 W Apache/2. 63 (Un
00440: C=200 10 L 37 W 586 Ch Apache/2.0.63 (Un
00430: C=301 9 L 30 W 333 Ch Apache/2.0.63 (Un
00470: C=301 9 L 30 W 329 Ch Apache/2.0.63 (Un
00620: C=301 9 L 30 W 330 Ch Apache/2.0.63 (Un
Hackers use programs called “Password Crackers” to find people’s passwords.


root@ubuntu: /mnt/hgfs/dev/linkedin
File Edit View Terminal Help
37b800aaea5541218850f5bed86691cdf2fd6ed2
ccbc00aaabce3f0c50381dcbf3568b4a514d61a2
c5bd00aa4b08ee49be6f8146db7a6ea27bfd513d
f9c300aa65330e3f3f1159181dd4b5a949a869f3
51d400aafe5607811af04c681317df364587d1d5
18dc00aa42b46ba9ced40e1ce2943dac3dc8ac51
cbe900aa3e6a5157c6b6b58d3b0871f736dbdef9
3eed00aa13b2984fa09be56a336dd6601d7930bb
77f800aaee4655bbd35dae2181000fa76479011e
000001aa34e8de87611a85359e59bdd642c655ba
000001aaa51879aeaf94db83ece85c7c3f280954
000001aa185f2e57aac09a6276bc54122e0dd875
000001aa95a820fd18856267a52fd494bf473f7b
000001aacf687a719d99755a7849fe5dc5c7ab7a
000001aacf8d46fc5302931b079b3c8ca733baf4
000001aa1ecc6caae2965f62d6e9592bab874779
000001aa8f26ef93374ed76870e090a044a30318
000001aa65850b48c3d3969b7a0a2b3d9d33587d
000001aad74f8bd5a135744fcd885b83300b519a
000001aaa763a9803fe629f4244385f039e0257a
000001aa90735cab45440f92e561bf406ec5e384
000001aa448b25f82543cff074476910194c02ad
000001aa3a5849fdcd1e661090d898b44ae9532f
000001aa236fd458da7fdf2ba71c729b5beff1a1
000001aa2b8357d9589130f5e0ff0255bb135a38
000001aa587bbce6f56c0c78039756a1b5cbf3d8
--More--
First password cracker trial:
Top 50 passwords
If yours is there:
Guessable in > 1 second!

Passwords
access
hello
iwantu
letmein
master
pass
password
please
qwerty
secret
trustno1

Names
*family
names

Numbers
1234
12345
123456
1234567
12345678
1111
111111
121212
123123
131313
2000
6969
696969
abc123

Keyboard
aaaaaa
abc123
asdfgh
qwerty

Superheros
batman
superman
cowboy

Colours
orange
purple
silver
yellow

Vulgar
biteme
*Body parts
*Swear words
*Things on HBO but not on CBC

Words
dragon
falcon
monkey
phoenix
tigger
iloveyou
love

Sports
baseball
football
golfer
hockey
soccer
yankees

Transport
camaro
corvette
Falcon
harley
mustang
porsche
ranger

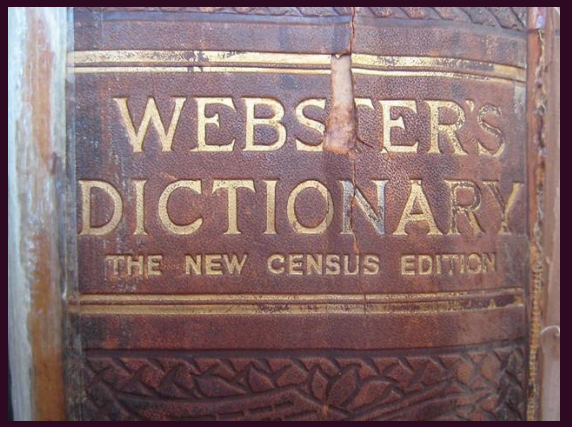
root@ubuntu: /mnt/hgfs/dev/linkedin

File Edit View Terminal Help

```
37b800aaea5541218850f5bed86691cdf2fd6ed2
ccbc00aaabce3f0c50381dcbf3568b4a514d61a2
c5bd00aa4b08ee49be6f8146db7a6ea27bfd513d
f9c300aa65330e3f3f1159181dd4b5a949a869f3
51d400aafe5607811af04c681317df364587d1d5
18dc00aa42b46ba9ced40e1ce2943dac3dc8ac51
cbe900aa3e6a5157c6b6b58d3b0871f736dbdef9
3eed00aa13b2984fa09be56a336dd6601d7930bb
77f800aaee4655bbd35dae2181000fa76479011e
000001aa34e8de87611a85359e59bdd642c655ba
000001aaa51879aeaf94db83ece85c7c3f280954
000001aa185f2e57aac09a6276bc54122e0dd875
000001aa95a820fd18856267a52fd494bf473f7b
000001aacf687a719d99755a7849fe5dc5c7ab7a
000001aacf8d46fc5302931b079b3c8ca733baf4
000001aa1ecc6caae2965f62d6e9592bab874779
000001aa8f26ef93374ed76870e090a044a30318
000001aa65850b48c3d3969b7a0a2b3d9d33587d
000001aad74f8bd5a135744fcd885b83300b519a
000001aaa763a9803fe629f4244385f039e0257a
000001aa90735cab45440f92e561bf406ec5e384
000001aa448b25f82543cff074476910194c02ad
000001aa3a5849fdcd1e661090d898b44ae9532f
000001aa236fd458da7fdf2ba71c729b5beff1a1
000001aa2b8357d9589130f5e0ff0255bb135a38
000001aa587bbce6f56c0c78039756a1b5cbf3d8
--More--
```

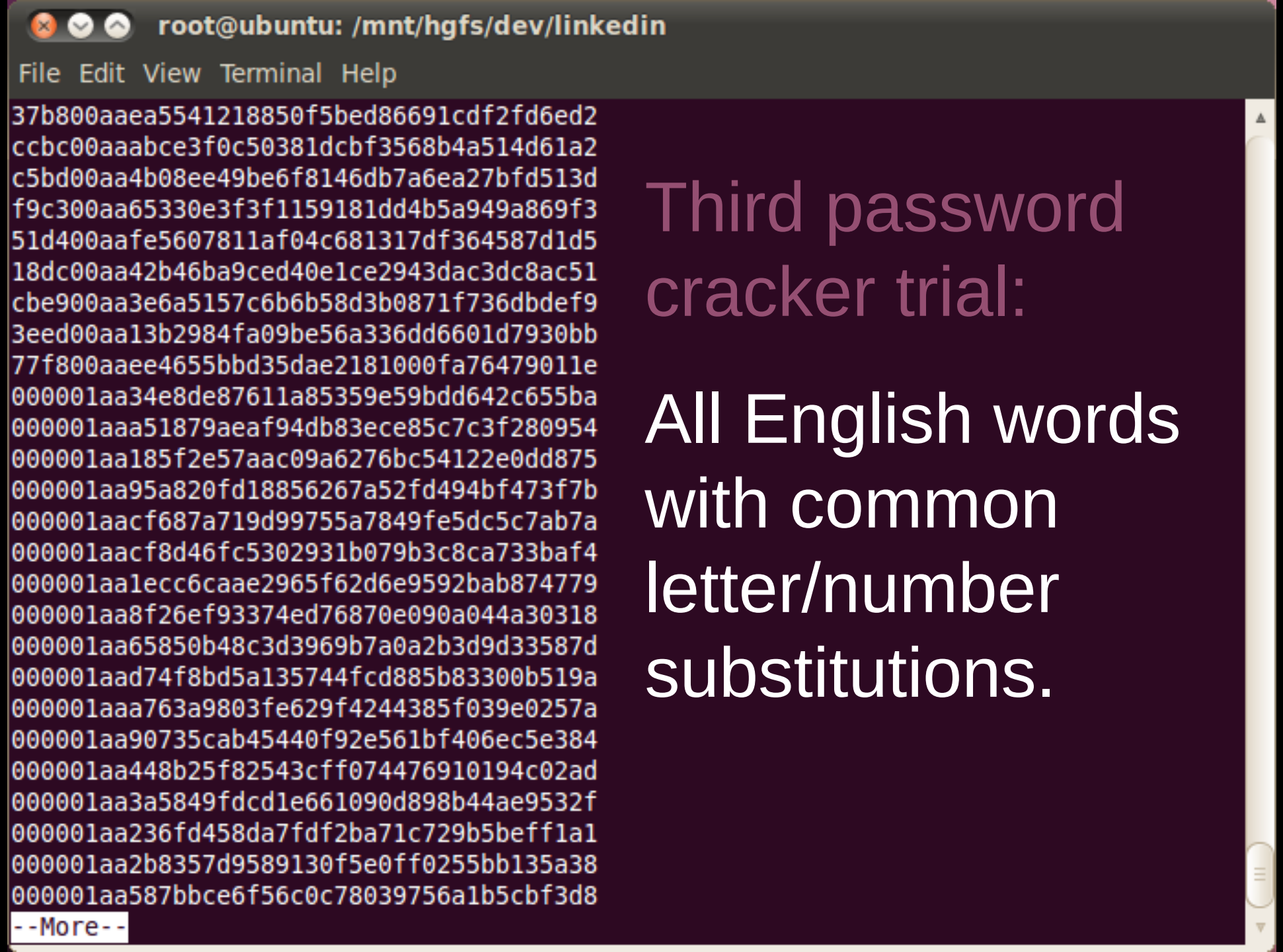
Second password cracker trial:

All words in dictionary



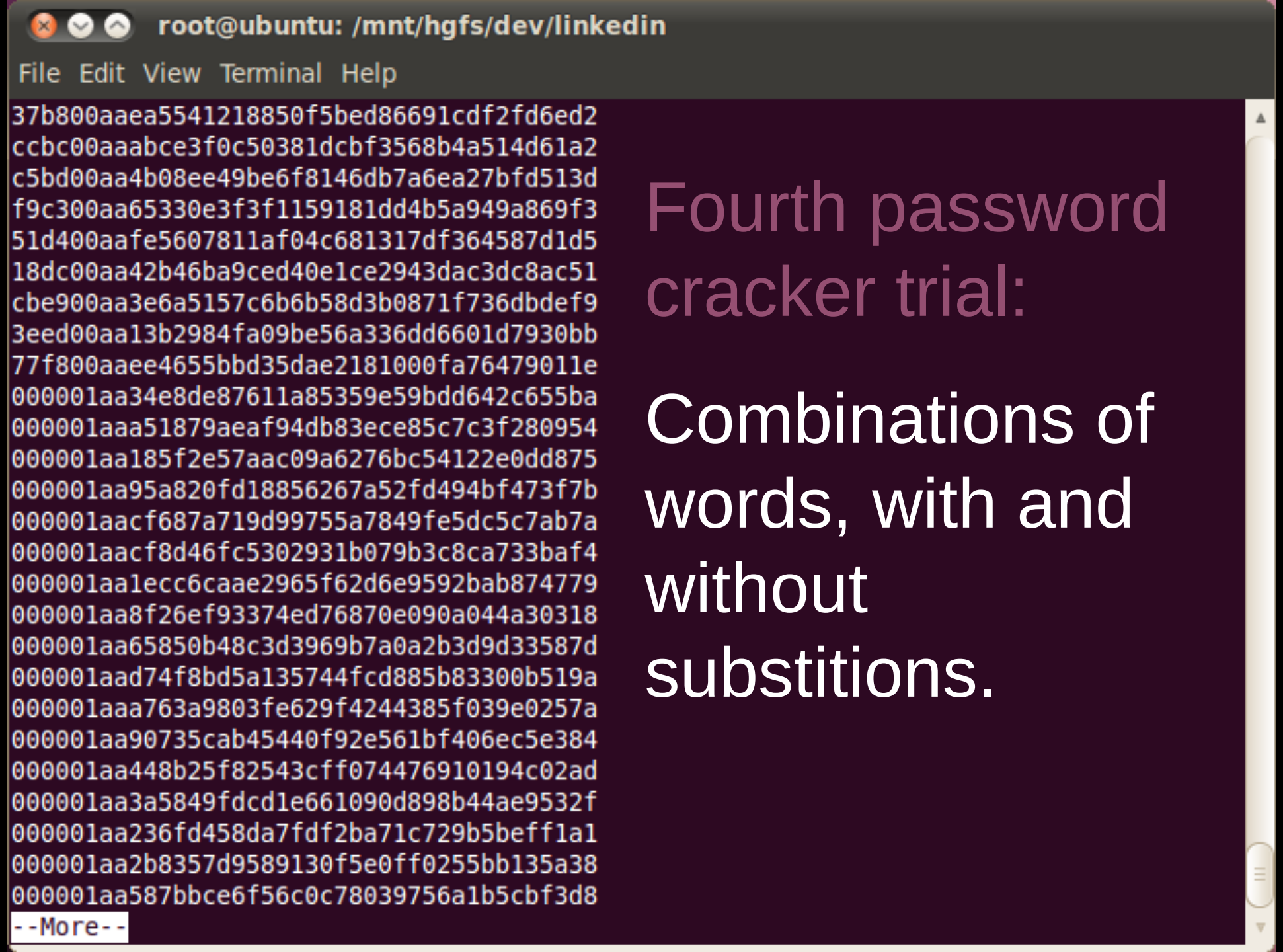
475,000 words.....

All guessable within 3 sec.



Third password cracker trial:

All English words with common letter/number substitutions.



Fourth password cracker trial:

Combinations of words, with and without substitions.

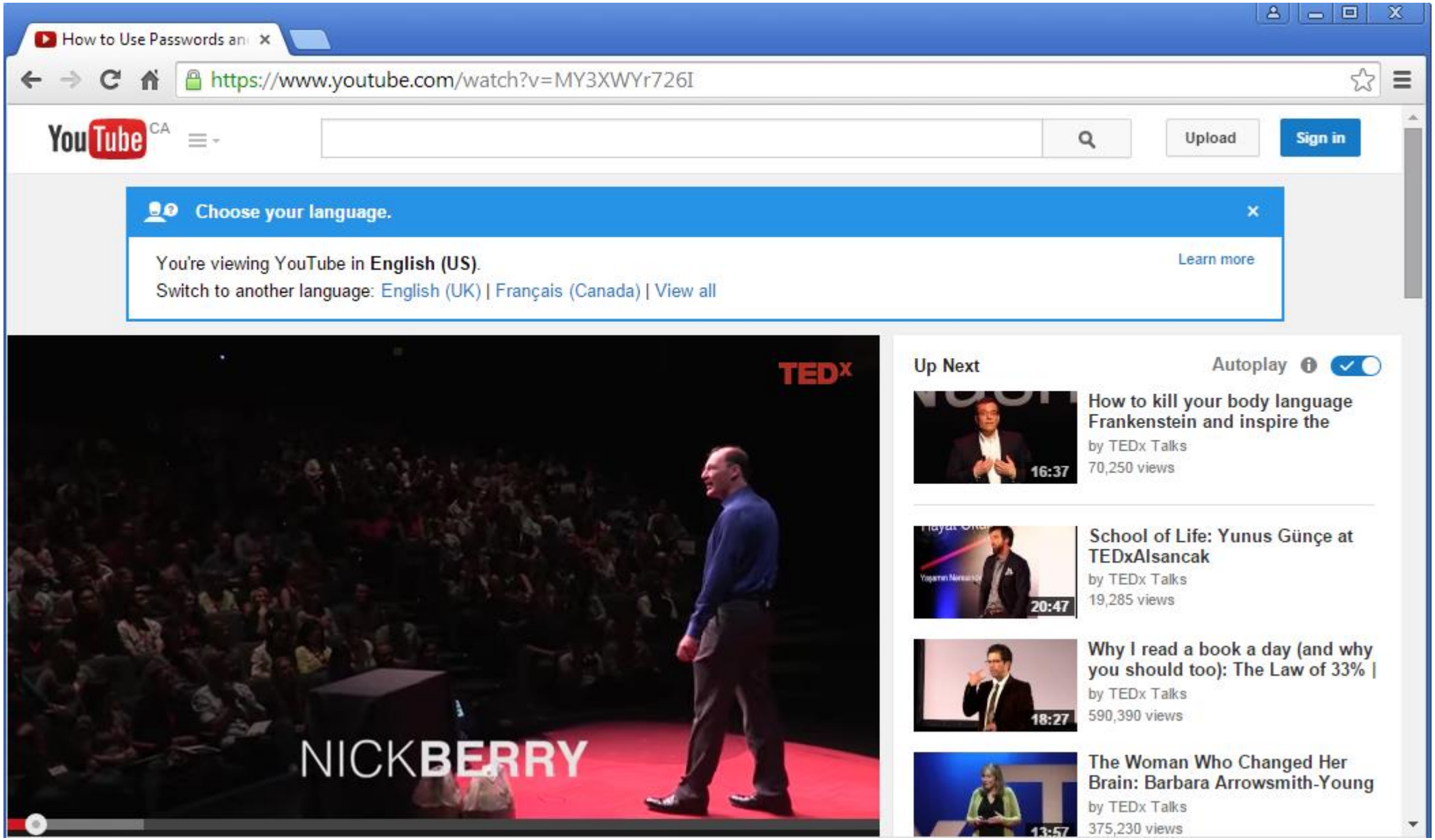
EPISODES - SEASON 46

@cbcmarketplace

BROADCAST DATE : SEP 28, 2018

Home Hack: How safe are your high-tech security devices?

The CBC hackers security tips.


How to Use Passwords an
https://www.youtube.com/watch?v=MY3XWYr726I
YouTube CA
Upload
Sign in
Choose your language.
You're viewing YouTube in English (US).
Switch to another language: English (UK) | Français (Canada) | View all
Learn more
TEDx
NICKBERRY
Up Next
Autoplay
How to kill your body language Frankenstein and inspire the
by TEDx Talks
70,250 views
16:37
School of Life: Yunus Günçe at TEDxAlsancak
by TEDx Talks
19,285 views
20:47
Why I read a book a day (and why you should too): The Law of 33% |
by TEDx Talks
590,390 views
18:27
The Woman Who Changed Her Brain: Barbara Arrowsmith-Young
by TEDx Talks
375,230 views

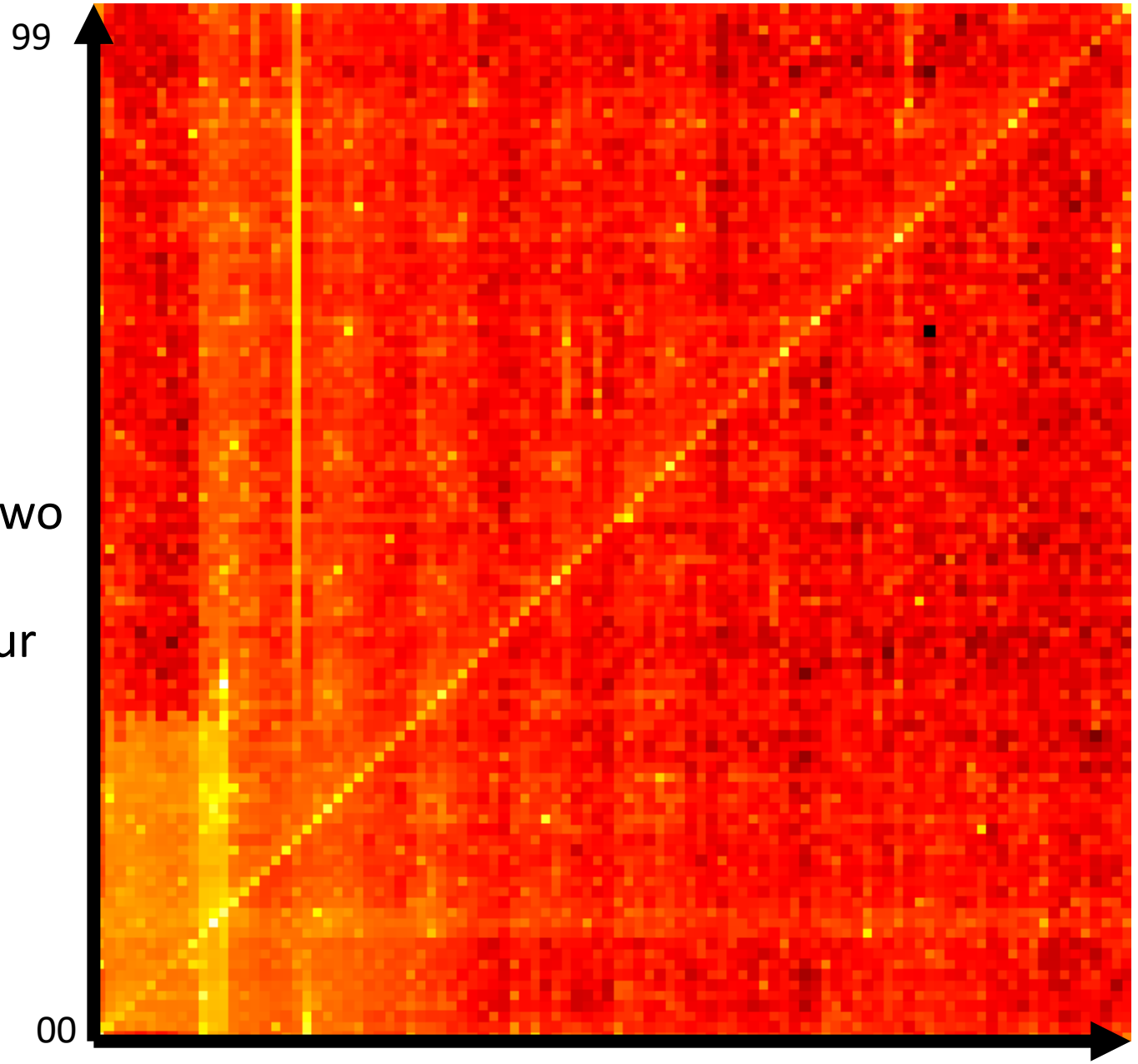
4 digit pin

10,000 possible combinations

However,
With 20 pins, you can hack 1/4 accounts
With 61 pins, you can hack 1/3 accounts
With 556 pins, you can hack 1/2 accounts

Top 20 Pins

1234	9999
1111	3333
0000	5555
1212	6666
7777	1122
1004	1313
2000	8888
4444	4321
2222	2001
6969	1010

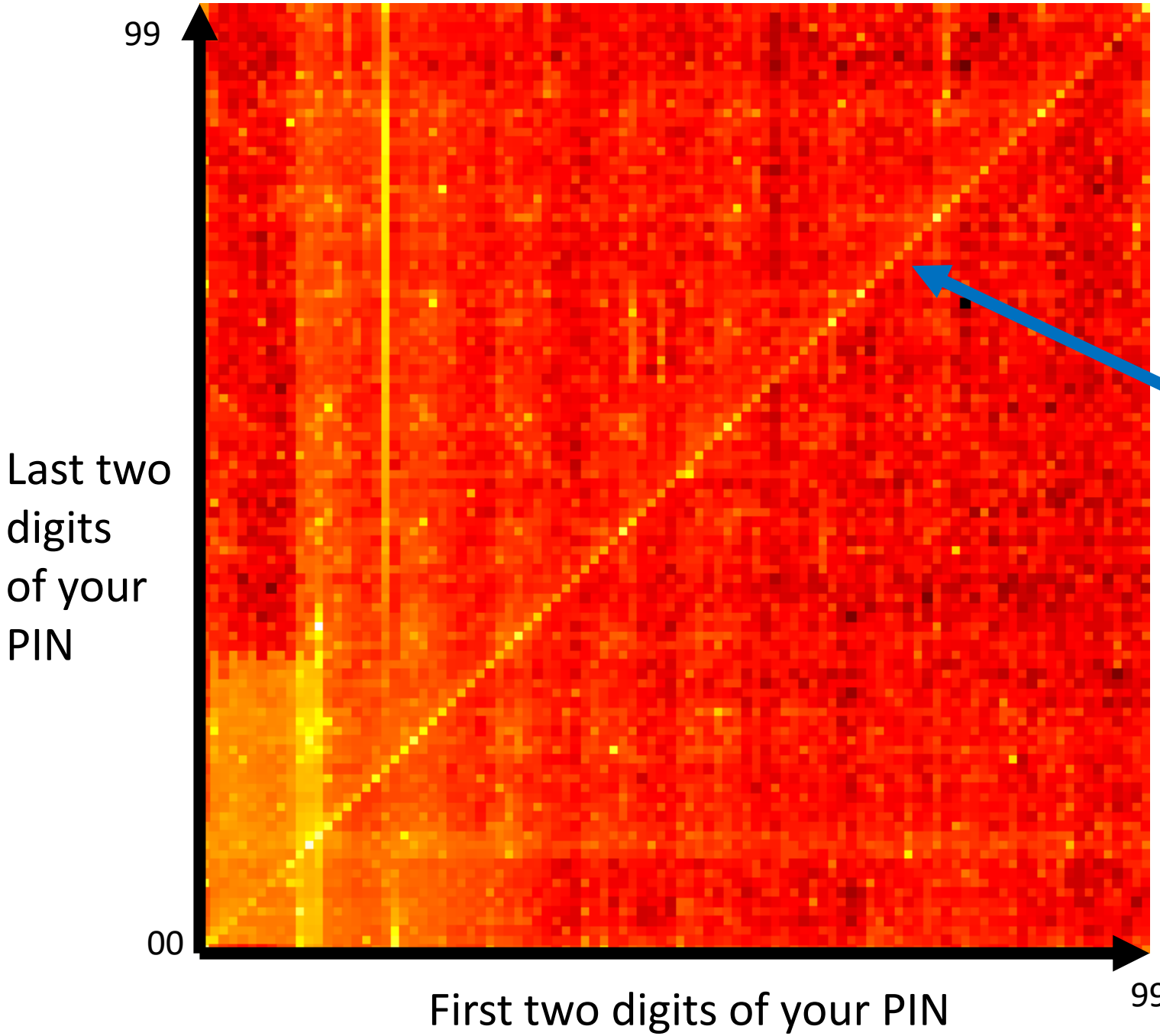


A PIN Heat Map

Yellow are more frequently used,
Red less frequently,
Brown and Black rarely.

http://www.datagenetics.com/blog/september32012/

If humans were good at picked random passwords, there would be no patterns in the data: The heat map would look like this box.



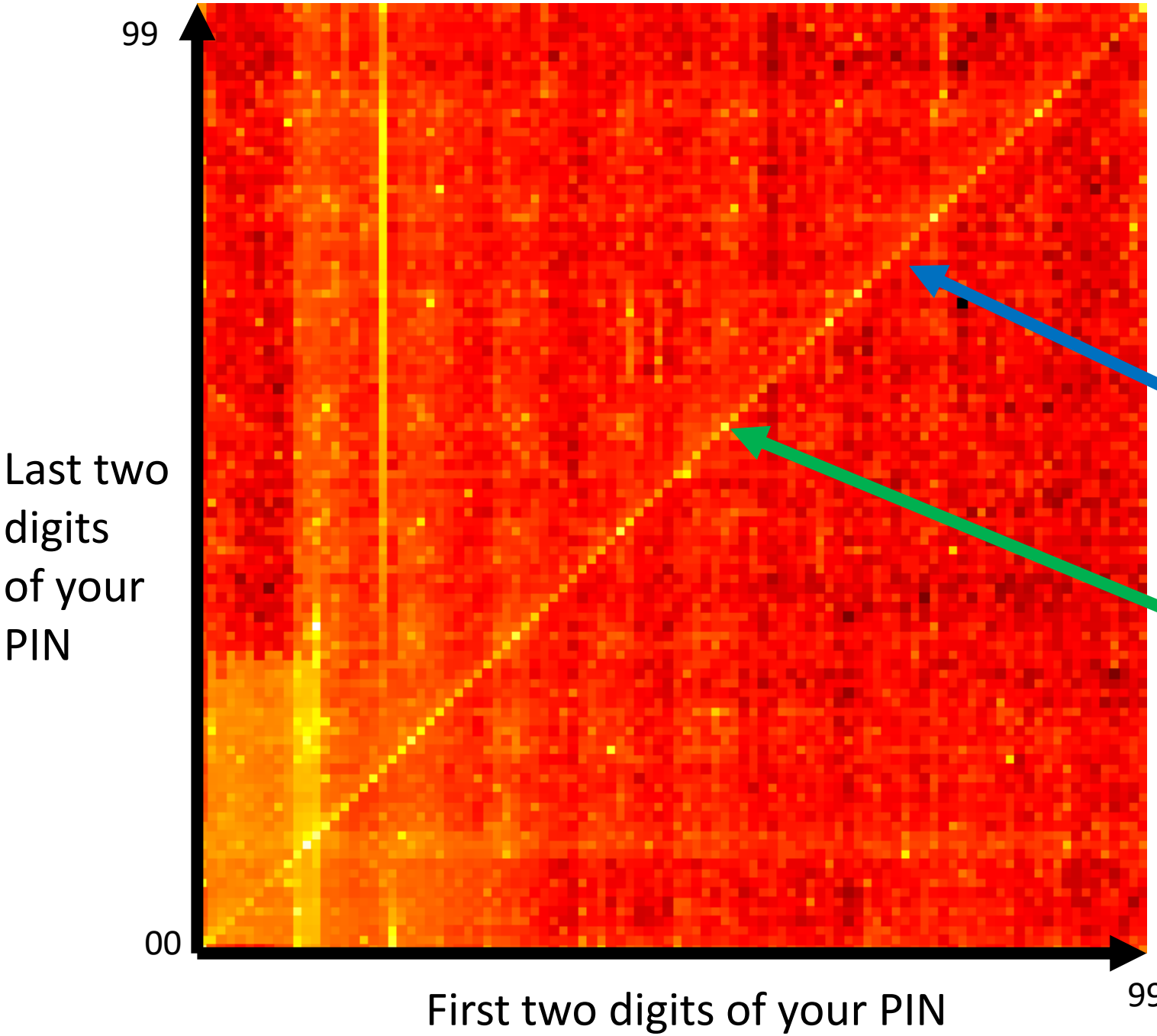
A PIN Heat Map

Yellow are more frequently used,
Red less frequently,
Brown and Black rarely.

Diagonal line,
Pairs of digits the same
1212 or 3434

A PIN Heat Map

Yellow are more frequently used,
Red less frequently,
Brown and Black rarely.

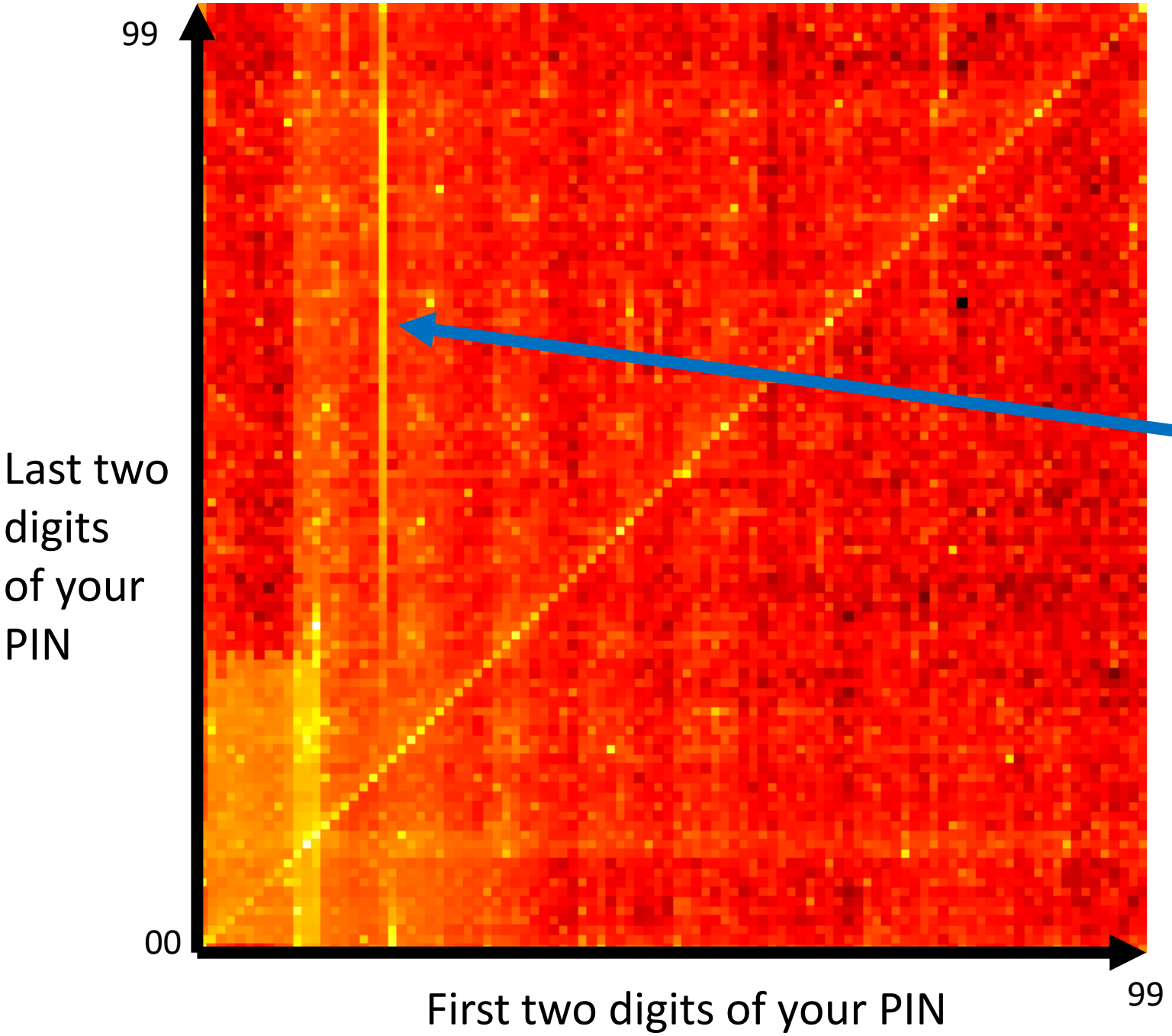


Diagonal line,
Pairs of digits the same
1212 or 3434

Every 11 dots,
One is extra bright.
All four digits the same

A PIN Heat Map

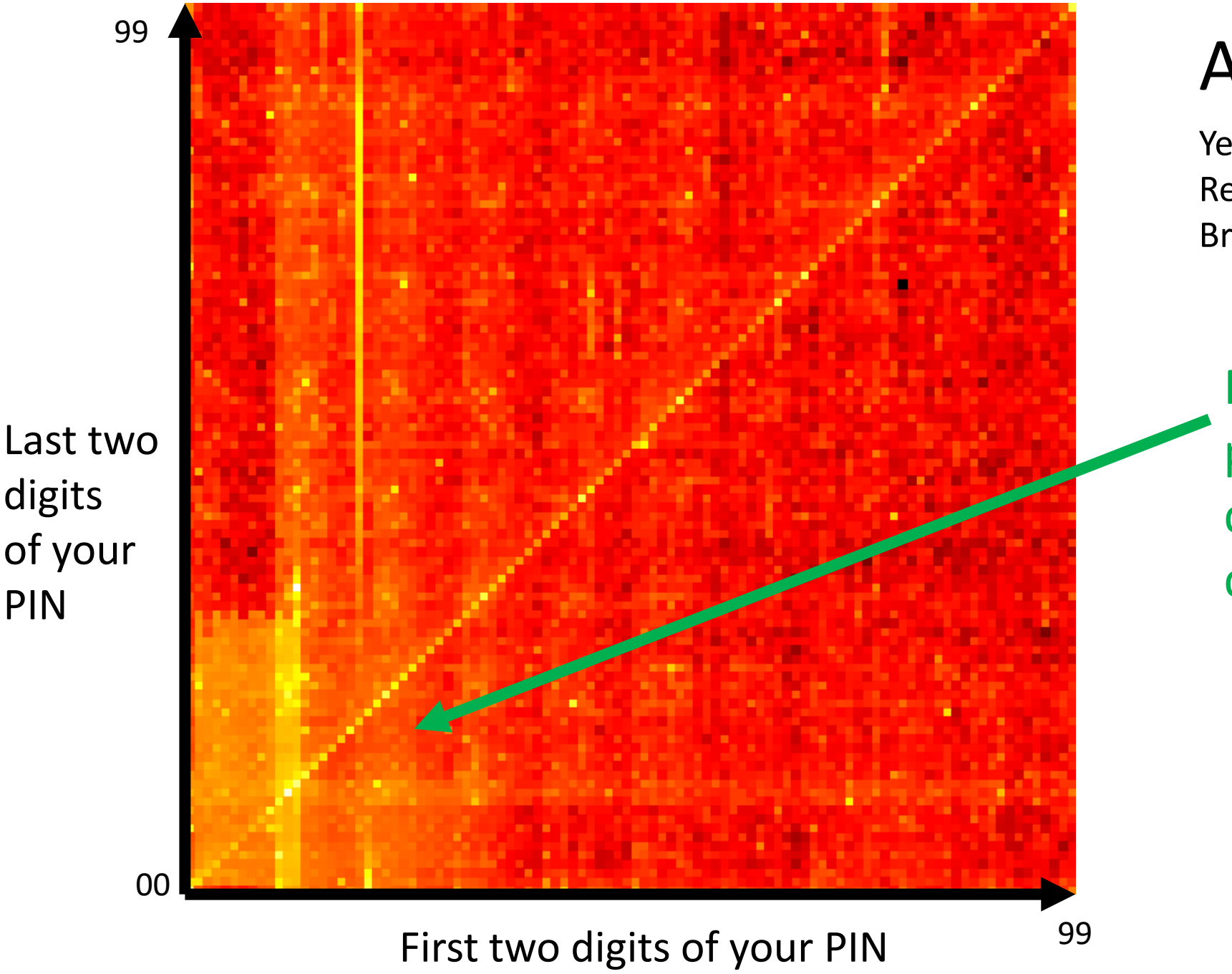
Yellow are more frequently used,
Red less frequently,
Brown and Black rarely.



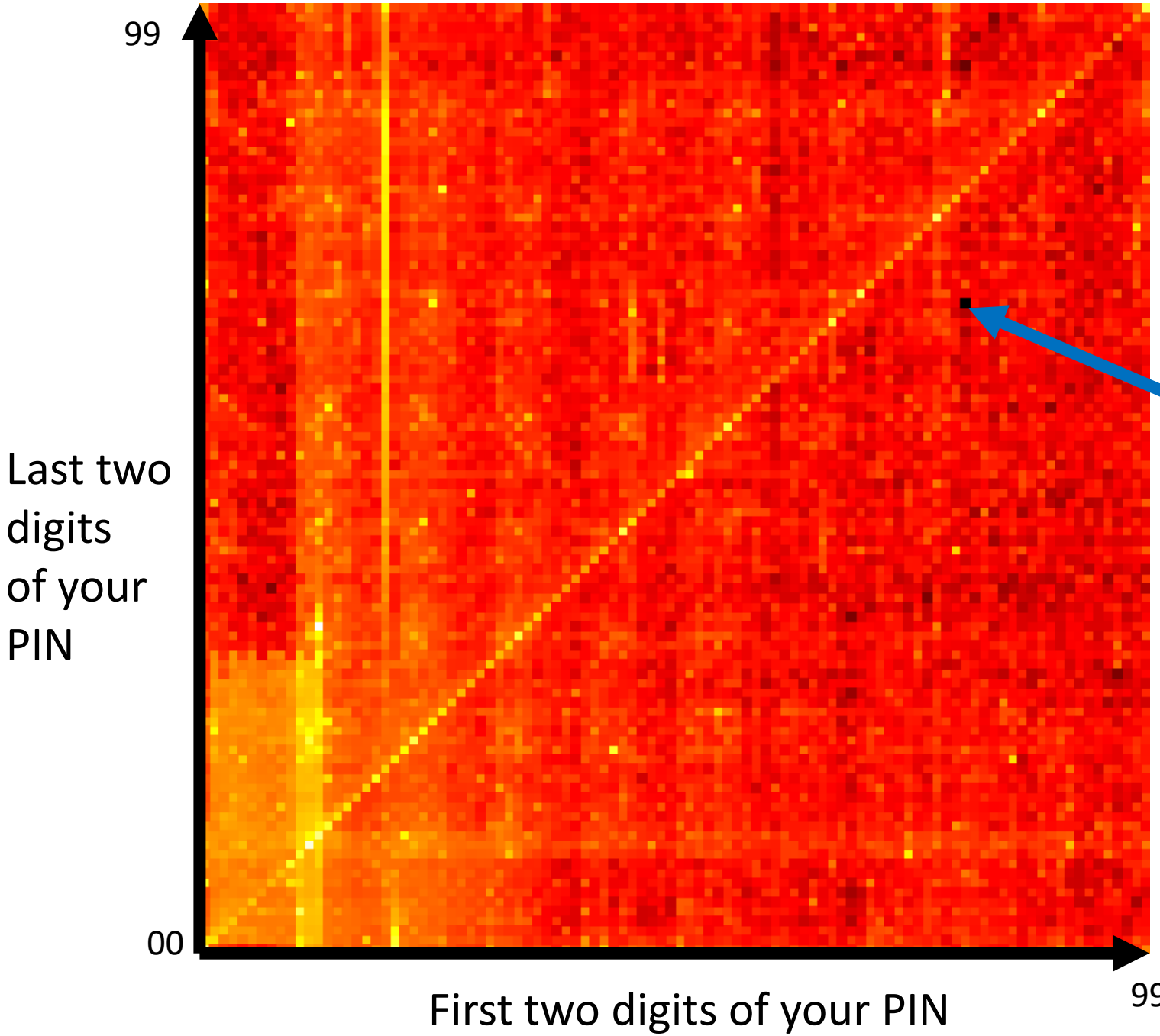
The line starting with 19XX,
These are people's birth years

A PIN Heat Map

Yellow are more frequently used,
Red less frequently,
Brown and Black rarely.



People who have picked mmdd or ddmm, significant dates.

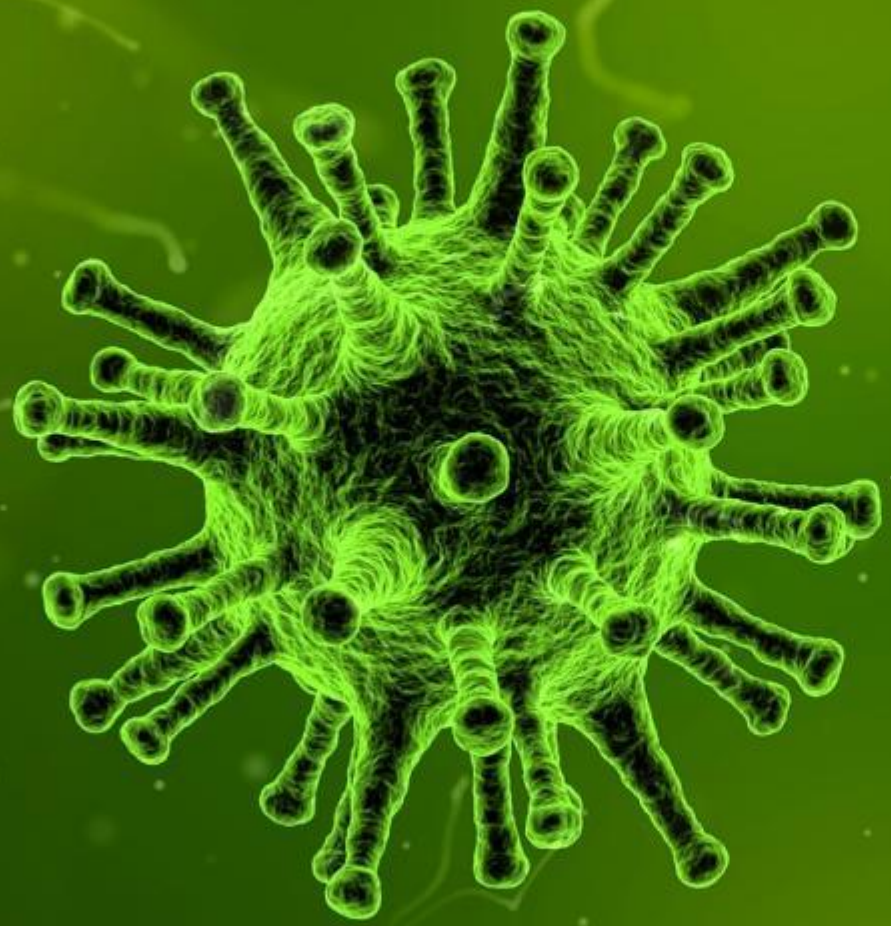


A PIN Heat Map

Yellow are more frequently used,
Red less frequently,
Brown and Black rarely.

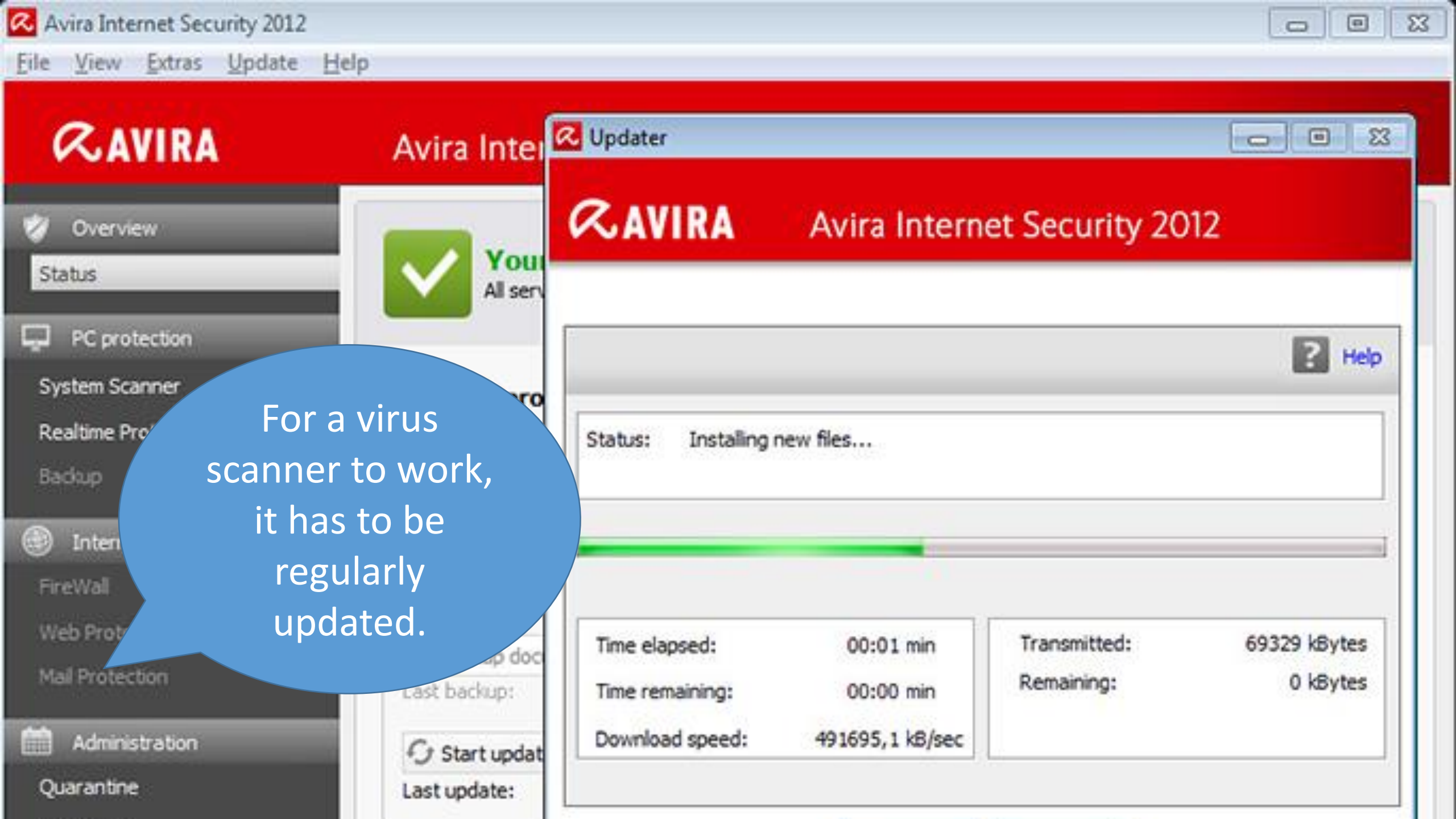
The least common pin is 8068


KASPERSKY lab
ANTI-VIRUS
Technical Preview
Cloud protection
Reports
Settings
Computer is protected
Threats: none
Protection components: enabled
Databases: have not been updated for a long time
License: 91 days remaining
Another good option is a virus scanner.
Scan
Update
Tools
Virtual Keyboard
Help
Support
My Kaspersky Account
Licensing

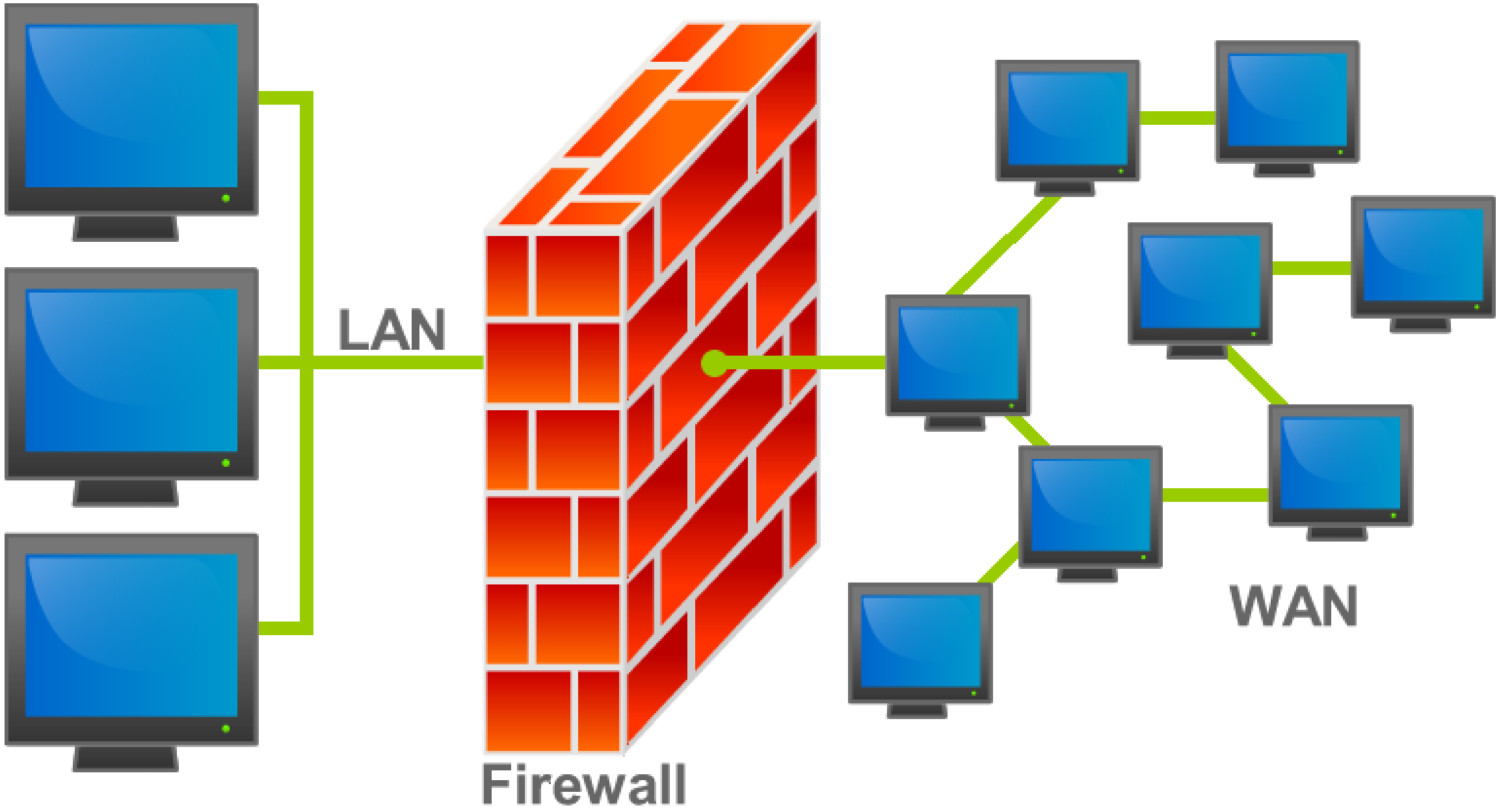


A virus scanner has a list of known viruses. It scans files to find matches of the code in it’s virus list.


VIRUS
DETECTED
Will catch common viruses. Better than nothing.


Avira Internet Security 2012
File View Extras Update Help
AVIRA
Overview
Status
PC protection
System Scanner
Backup
Administration
Quarantine
Updater
AVIRA
Avira Internet Security 2012
Help
Status: Installing new files...
Time elapsed: 00:01 min
Time remaining: 00:00 min
Download speed: 491695,1 kB/sec
Transmitted: 69329 kBytes
Remaining: 0 kBytes
Start updat
Last update:
For a virus scanner to work, it has to be regularly updated.

Can’t catch any zero-day attacks. Those haven’t been discovered yet.


LAN
Firewall
WAN

A firewall scans all incoming internet traffic for viruses.

It is, in effect, a virus scanner.


Security experts estimate that only 10% of viruses are caught by virus scanners and firewalls.
Mikko Hypponen, F-secure


The Pentagon has a reverse scanner: Einstein. It only allows in files that are on a “good” list.

Network Use

Filled with viruses.

Many companies don’t allow you to use them at work to protect the servers.

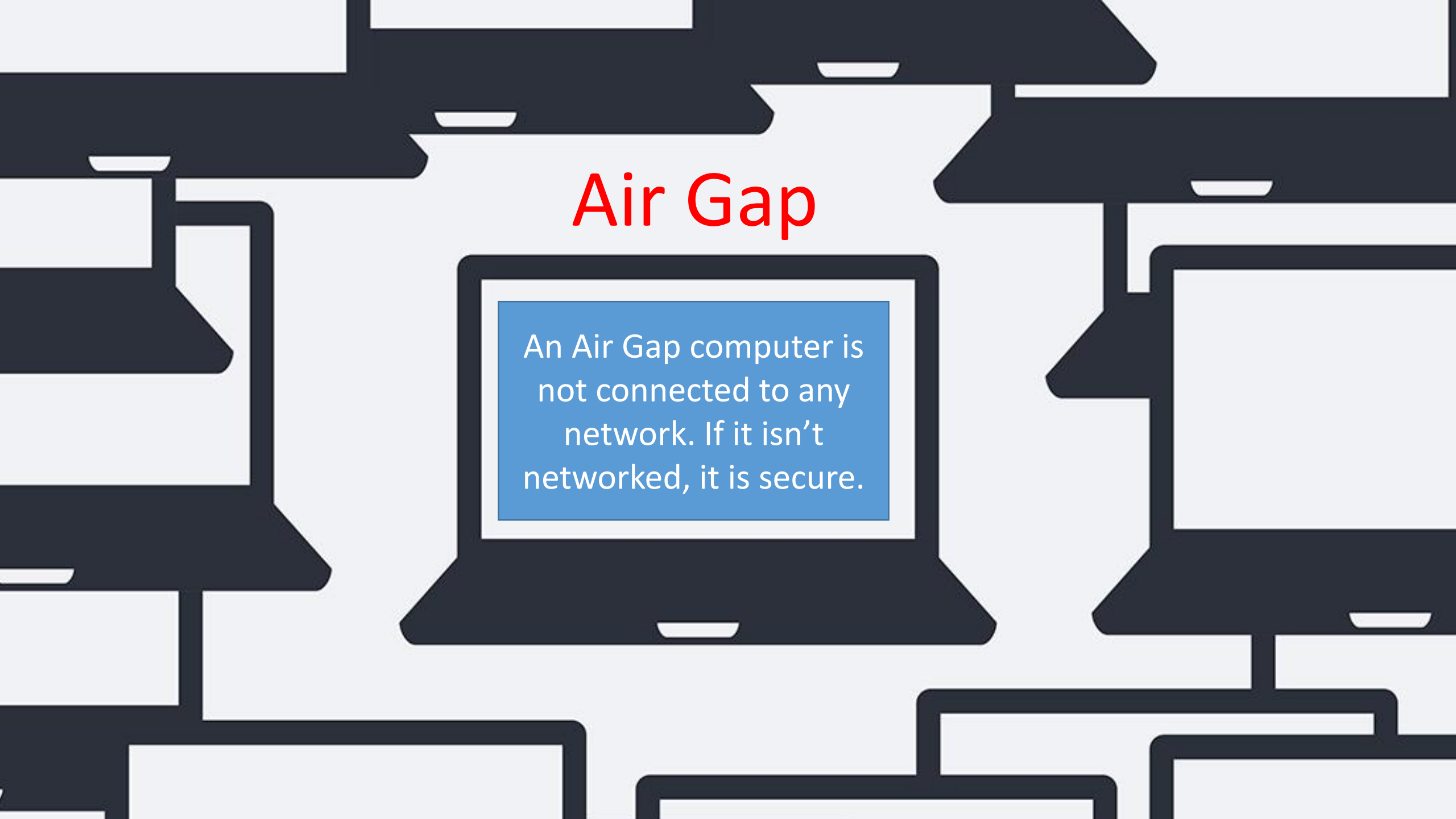
Peel's Password Rules

- Can't contain your name
- Can't contain your birthday
- Can't contain an old password
- Must have a capital letter
- Must have an odd character
- Must have a number


Some companies don’t allow their employees to use USBs. Why?


Not following a Network Use Policy is grounds for immediate dismissal.

Air Gap

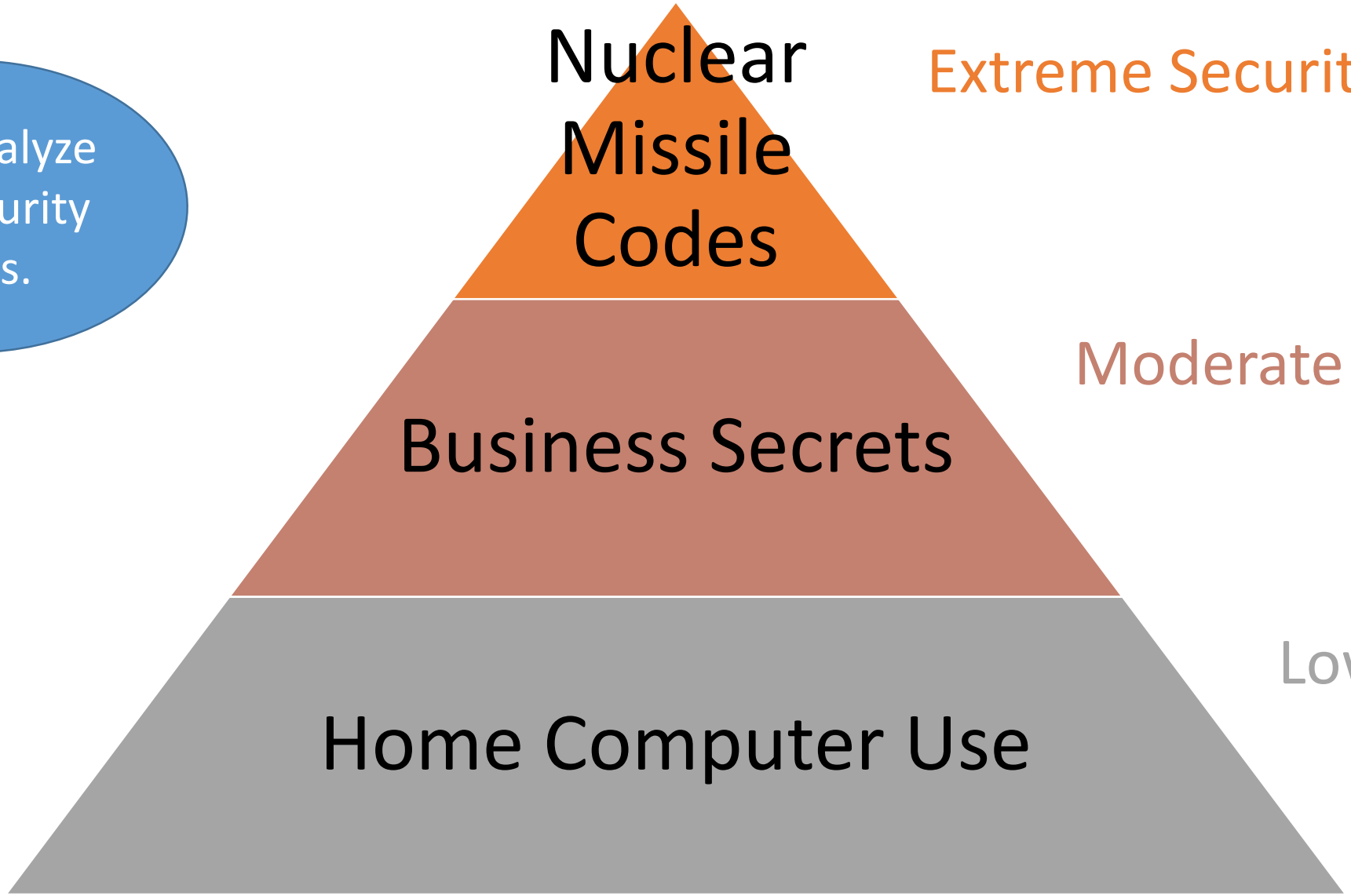

An Air Gap computer is not connected to any network. If it isn’t networked, it is secure.


Unicorns and Air Gaps – Do They Really Exist?
Living with Reality in Critical Infrastructures
Eric Byres, P.Eng.
CTO and VP Engineering, Tofino Security
Part of Belden Inc.
HIRSCHMANN
A BELDEN BRAND
TOFINO

Nuclear Missile Launch Codes

Risk Assessment Pyramid

Let's analyze the Security levels.

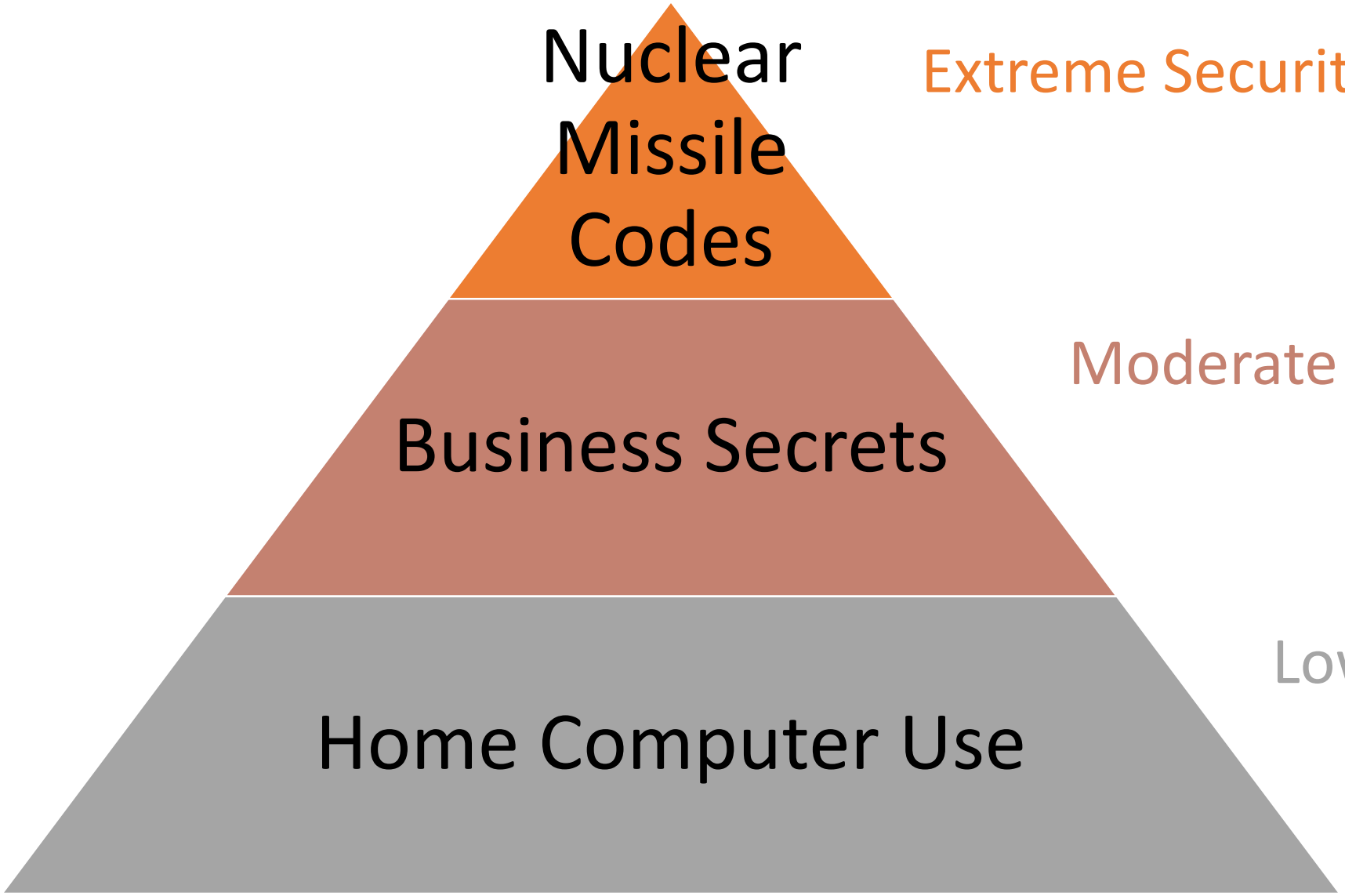


Extreme Security

Moderate Security

Low Security

Risk Assessment Pyramid



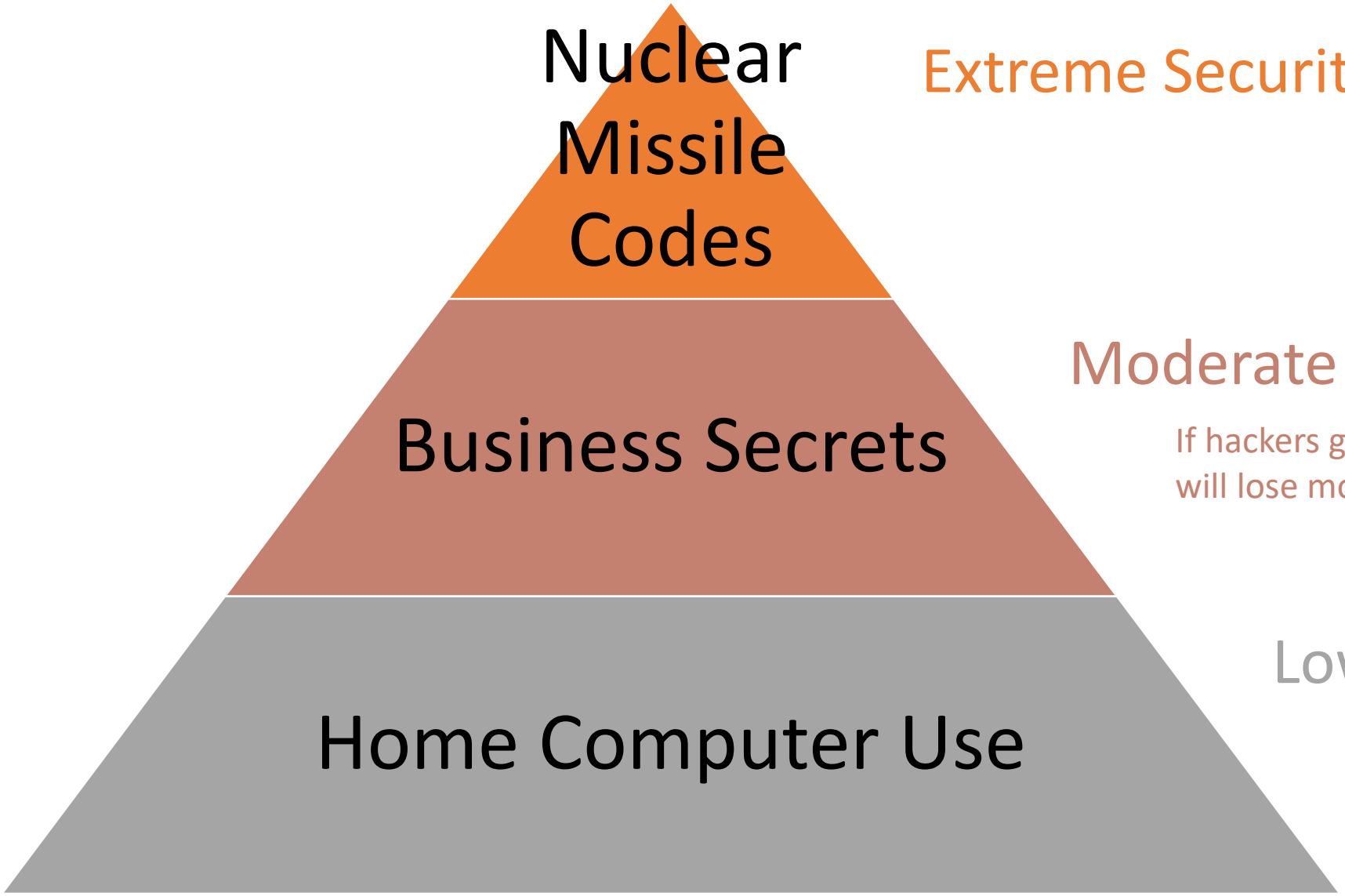
Extreme Security

Moderate Security

Low Security

If hackers get in, your identity might get stolen.

Risk Assessment Pyramid



Extreme Security

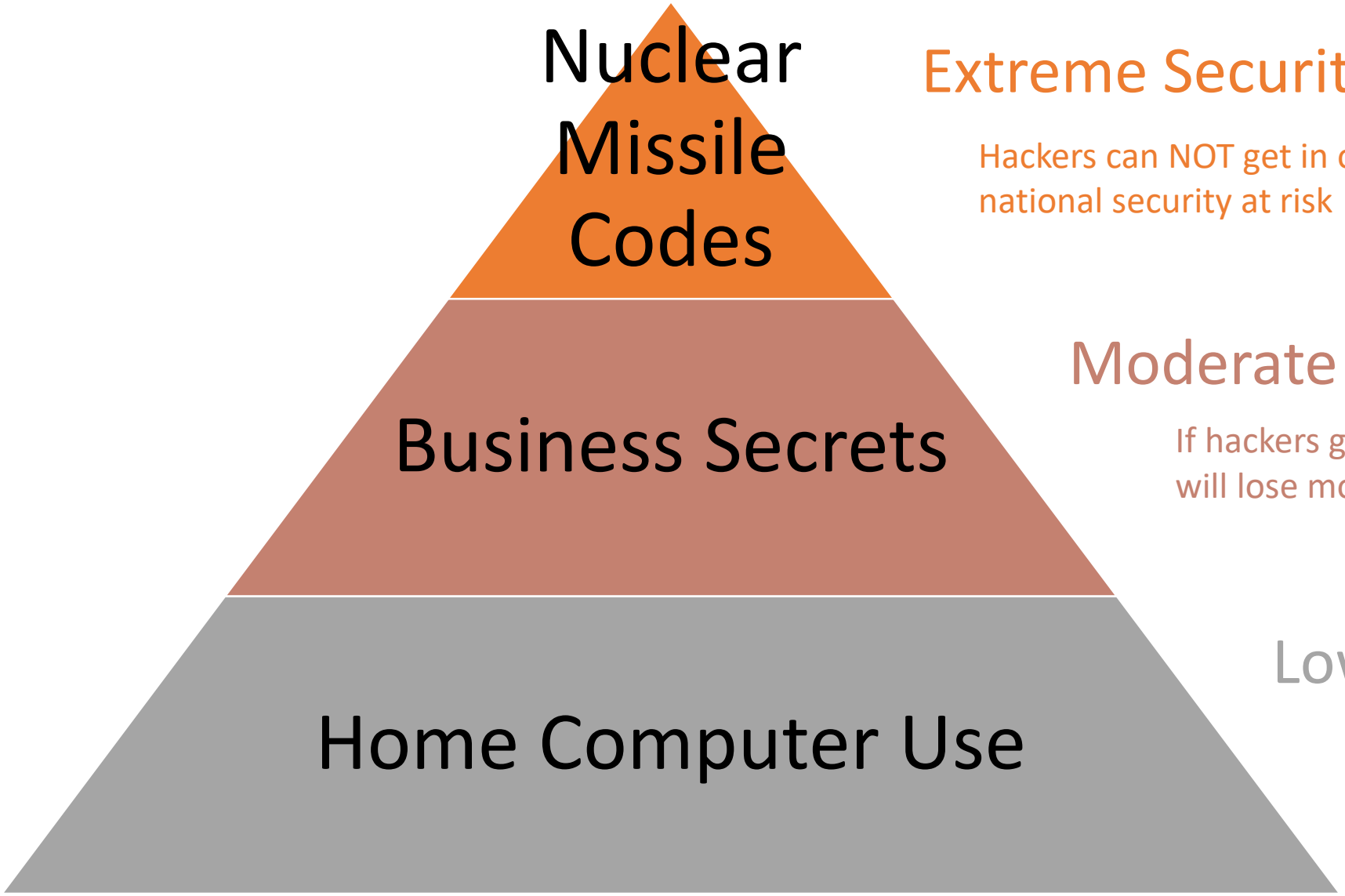
Moderate Security

If hackers get in, business will lose money

Low Security

If hackers get in, your identity might get stolen.

Risk Assessment Pyramid



Extreme Security

Hackers can NOT get in or national security at risk

Moderate Security

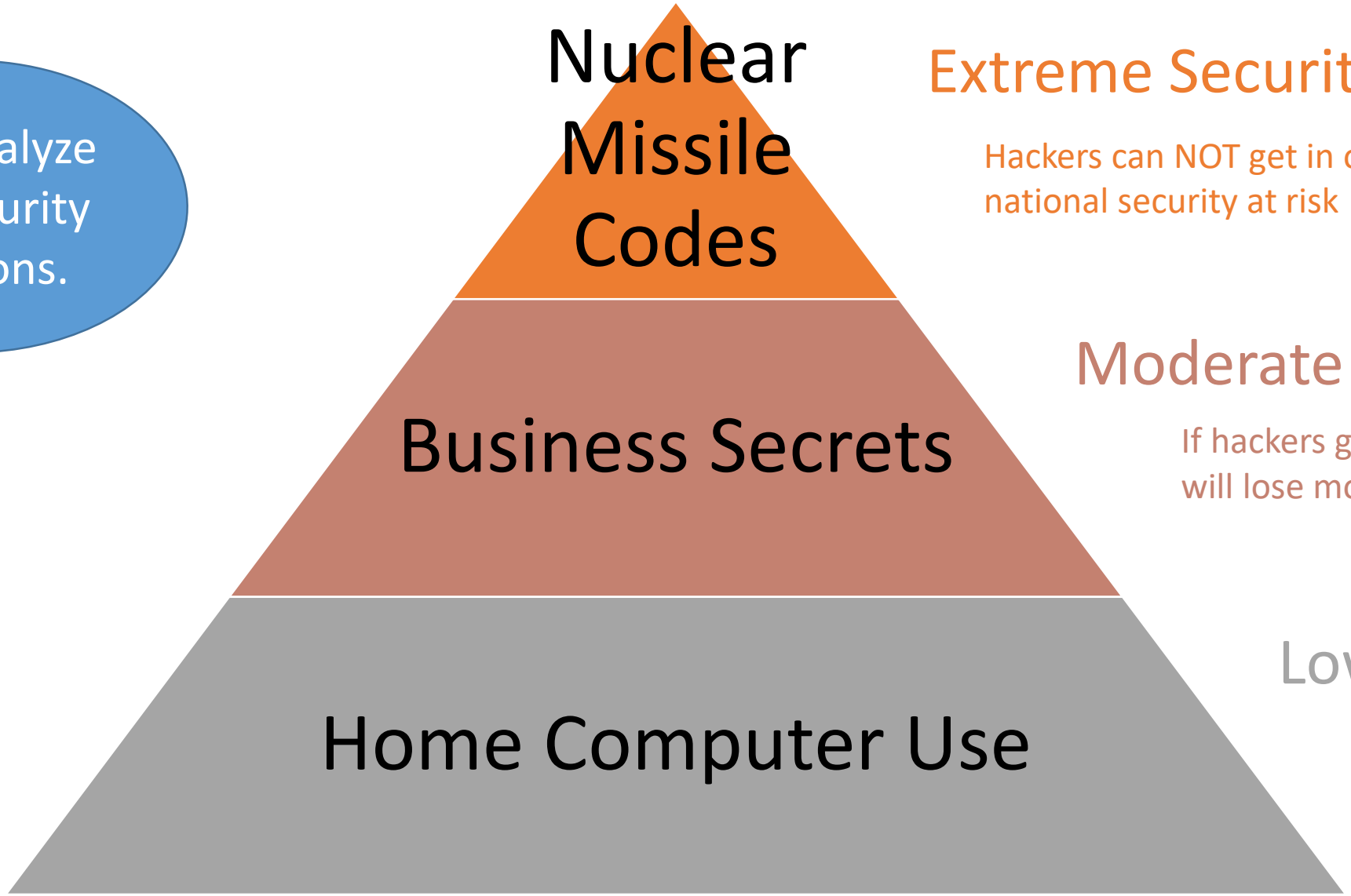
If hackers get in, business will lose money

Low Security

If hackers get in, your identity might get stolen.

Risk Assessment Pyramid

Let's analyze the Security Solutions.



Extreme Security

Hackers can NOT get in or national security at risk

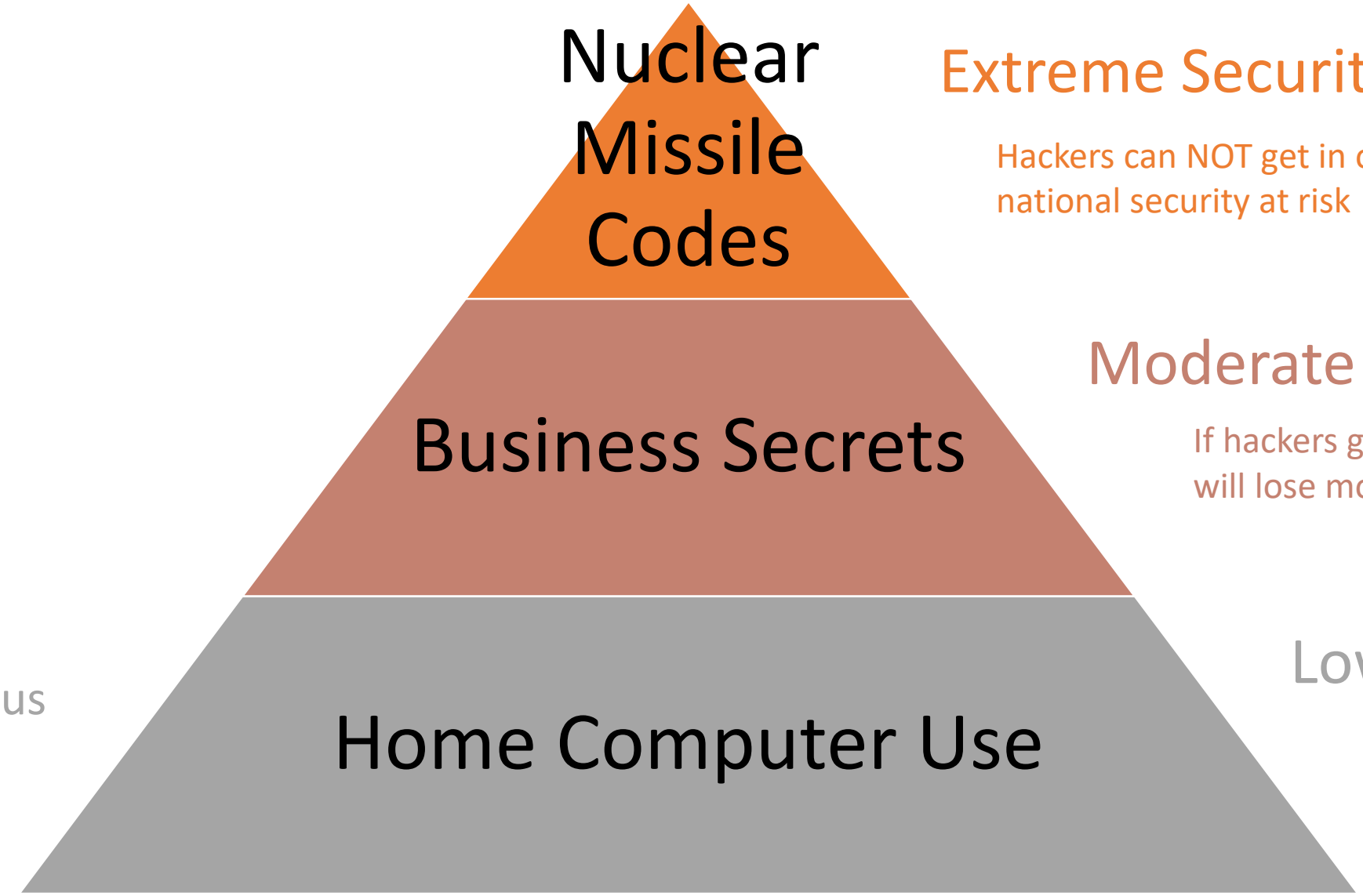
Moderate Security

If hackers get in, business will lose money

Low Security

If hackers get in, your identity might get stolen.

Risk Assessment Pyramid



Extreme Security

Hackers can NOT get in or national security at risk

Moderate Security

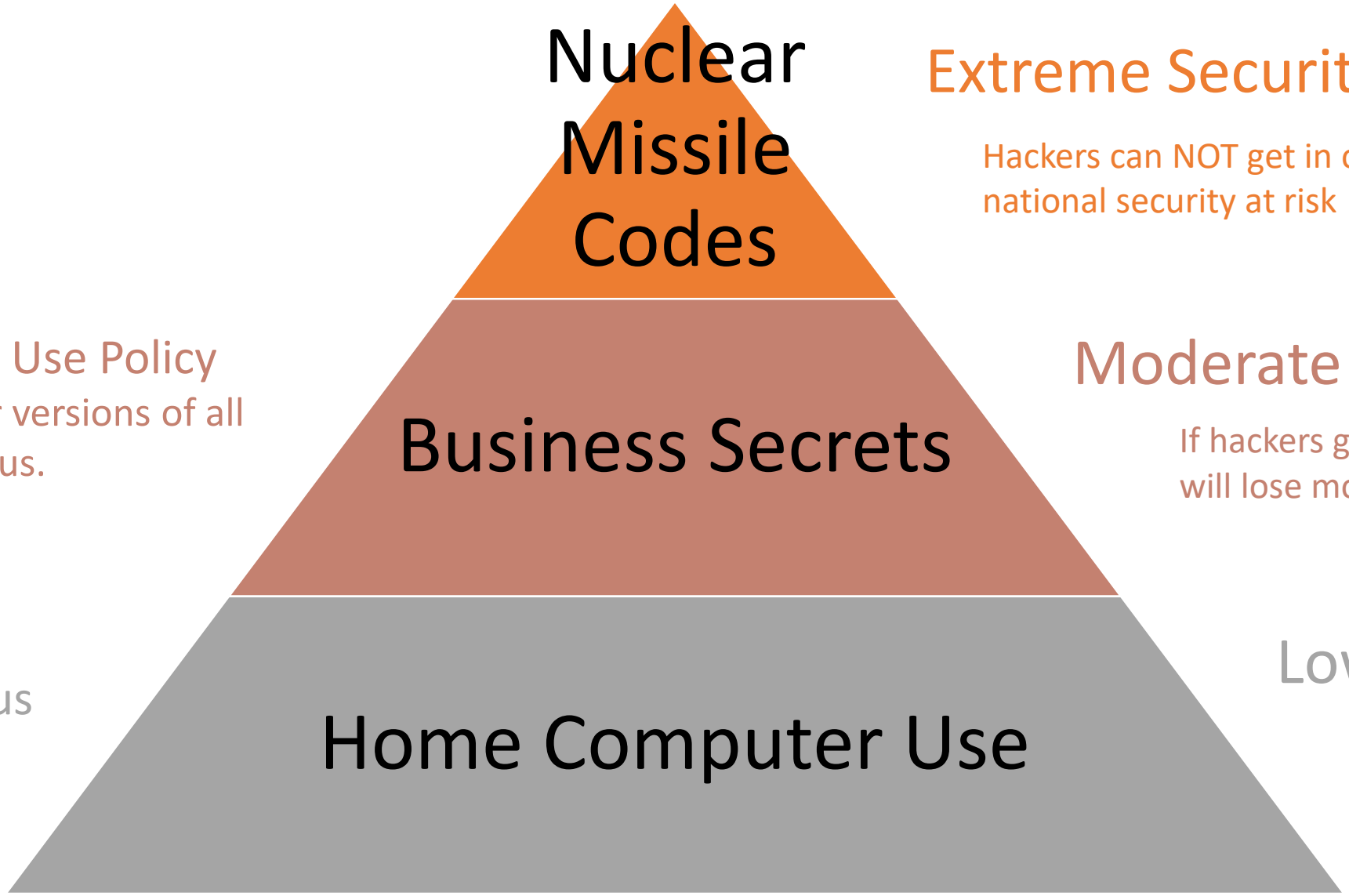
If hackers get in, business will lose money

Low Security

If hackers get in, your identity might get stolen.

Passwords, Firewall, Virus Scanner.

Risk Assessment Pyramid



Extreme Security

Hackers can NOT get in or national security at risk

Moderate Security

If hackers get in, business will lose money

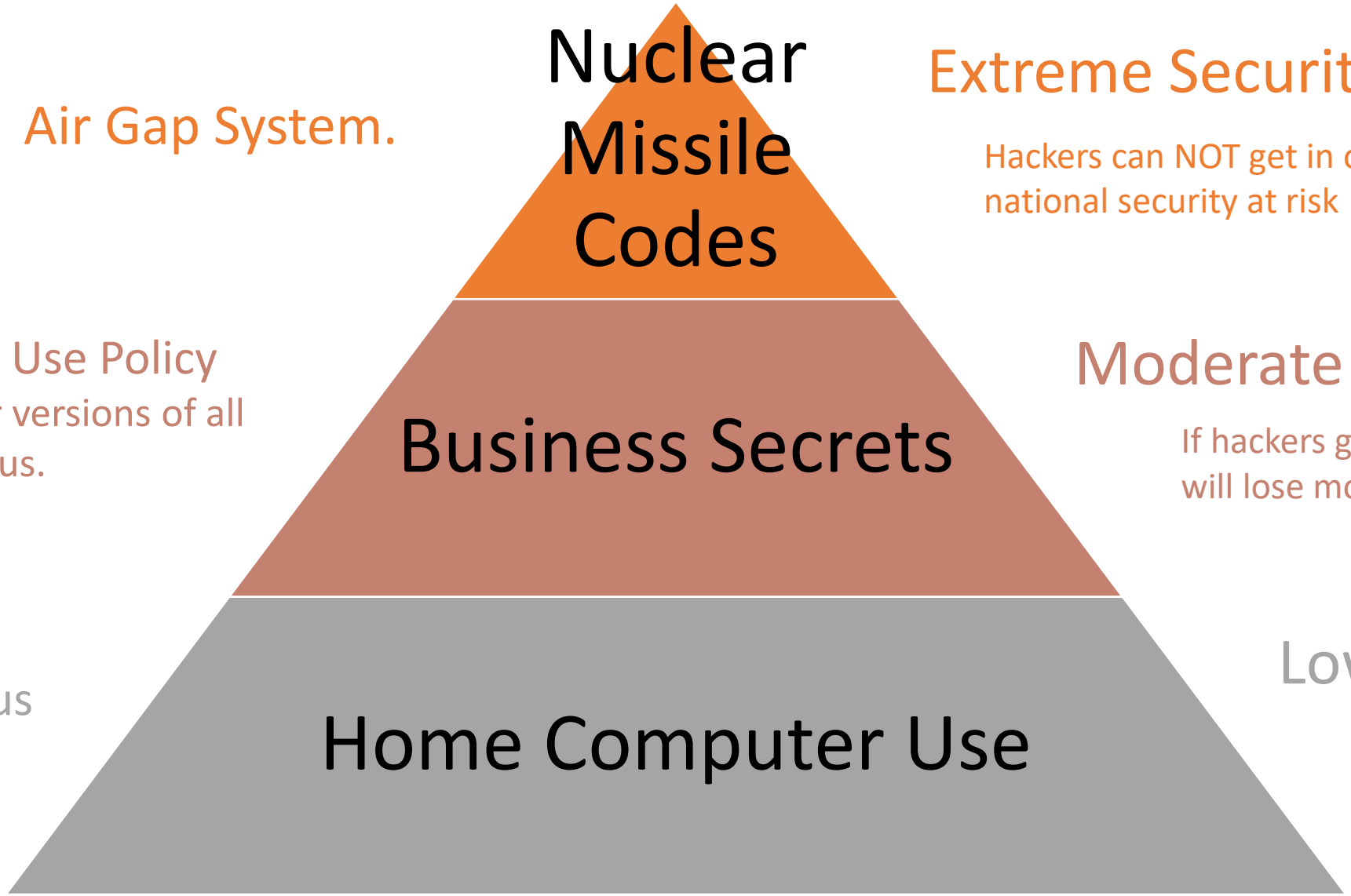
Low Security

If hackers get in, your identity might get stolen.

Network Use Policy and better versions of all the previous.

Passwords, Firewall, Virus Scanner.

Risk Assessment Pyramid



Air Gap System.

Extreme Security

Hackers can NOT get in or national security at risk

Network Use Policy and better versions of all the previous.

Moderate Security

If hackers get in, business will lose money

Passwords, Firewall, Virus Scanner.

Low Security

If hackers get in, your identity might get stolen.

Remember:
when the internet was designed, they choose speed over security.

That means that all security solutions slow down the internet. The more security you have, the slower the internet is.

With the case of the Air Gap, the internet isn’t just slow, you are no longer connected to it.

Air Gap Systems trade connectivity for extreme security.

Security Solutions

2.10C

For each security level, name some computer security methods that could be used.
(Work Bank: Air Gap, Password, Backup, Virus Scanner, Firewall, Network Use Policy)

Low security required	Moderate security required	Very high security required
Home Computer Use	Business Computer Use	Military Weapons
1. password 2. backups 3. virus scanner 4. firewall	1. network use policy *And better versions of:* 2. password 3. backups 4. virus scanner 5. firewall	1. air gap

Only 10% of viruses are caught with a virus scanner or firewall; however that is better than nothing!