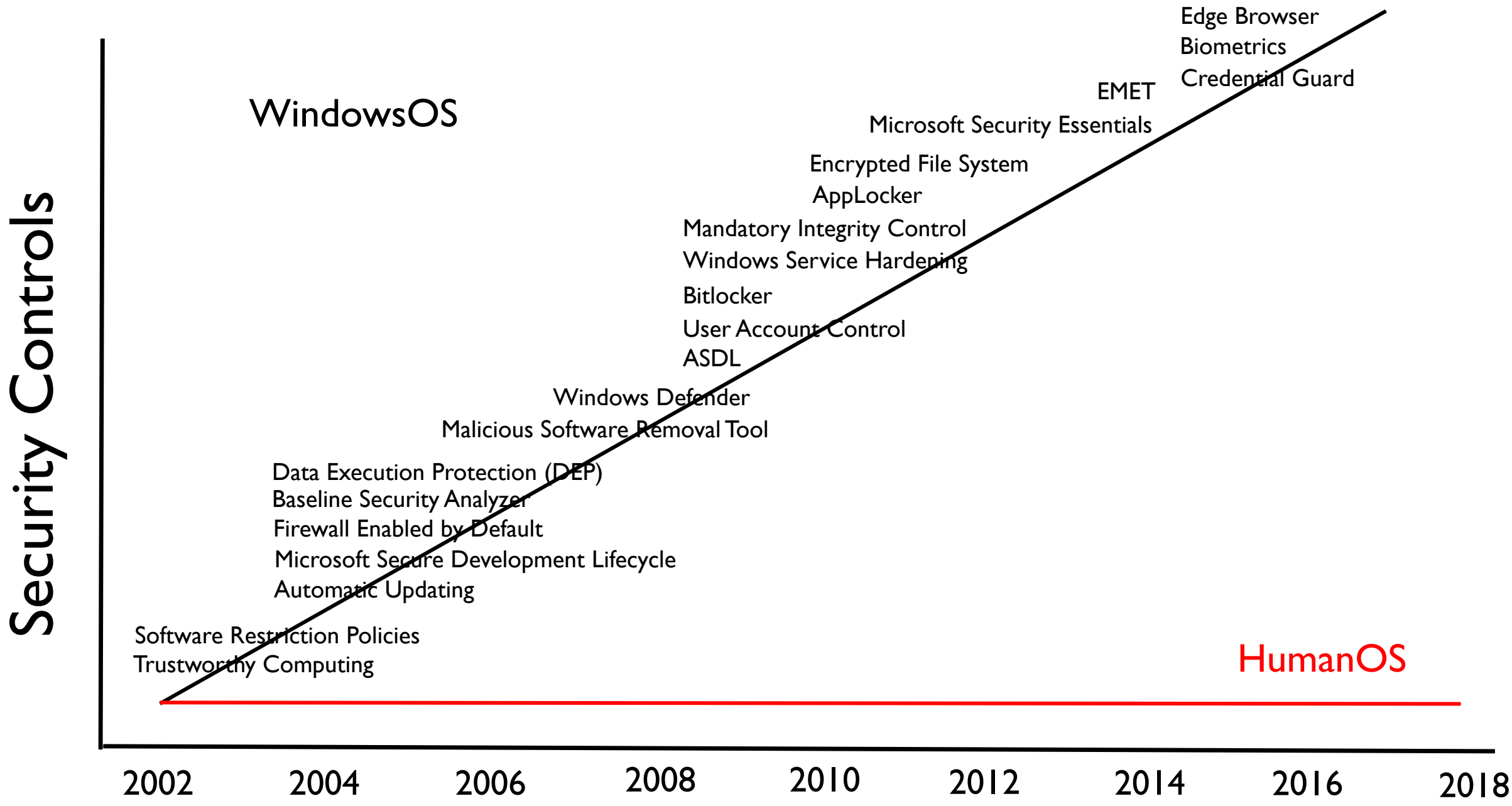
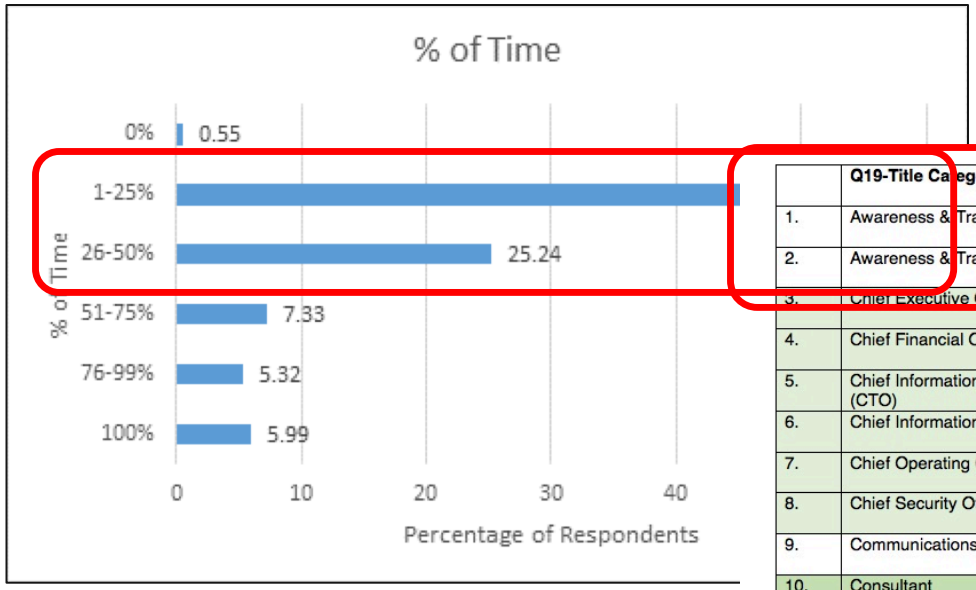
Making Security Simple

Lance Spitzner

@lspitzner

SANS SECURITY AWARENESS

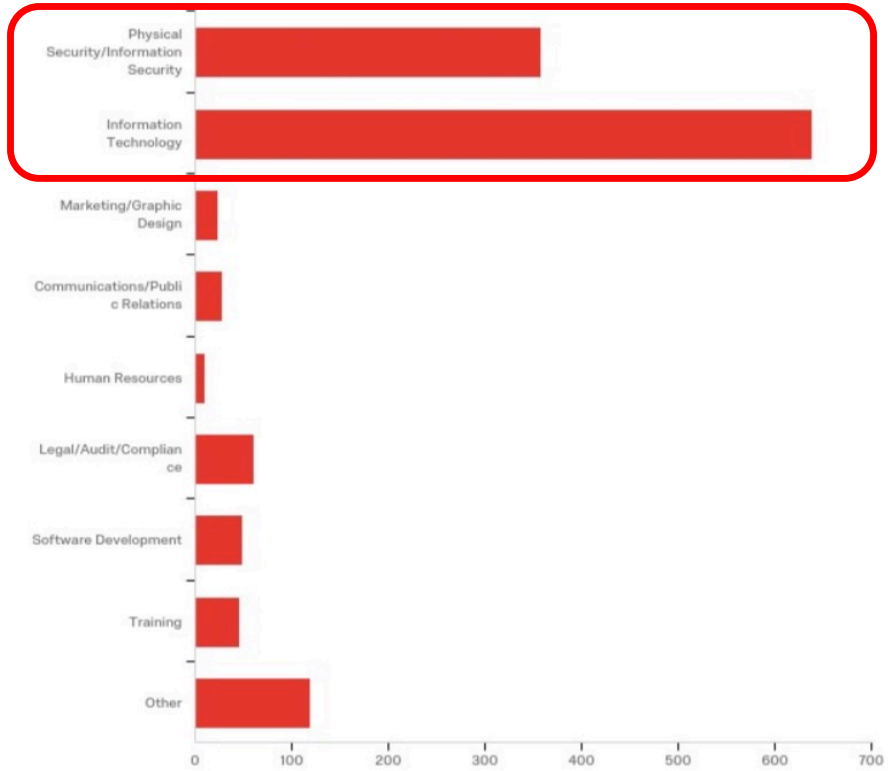

Security Controls
WindowsOS
Edge Browser
Biometrics
Credential Guard
EMET
Microsoft Security Essentials
Encrypted File System
AppLocker
Mandatory Integrity Control
Windows Service Hardening
Bitlocker
User Account Control
ASDL
Windows Defender
Malicious Software Removal Tool
Data Execution Protection (DEP)
Baseline Security Analyzer
Firewall Enabled by Default
Microsoft Secure Development Lifecycle
Automatic Updating
Software Restriction Policies
Trustworthy Computing
HumanOS
2002
2004
2006
2008
2010
2012
2014
2016
2018



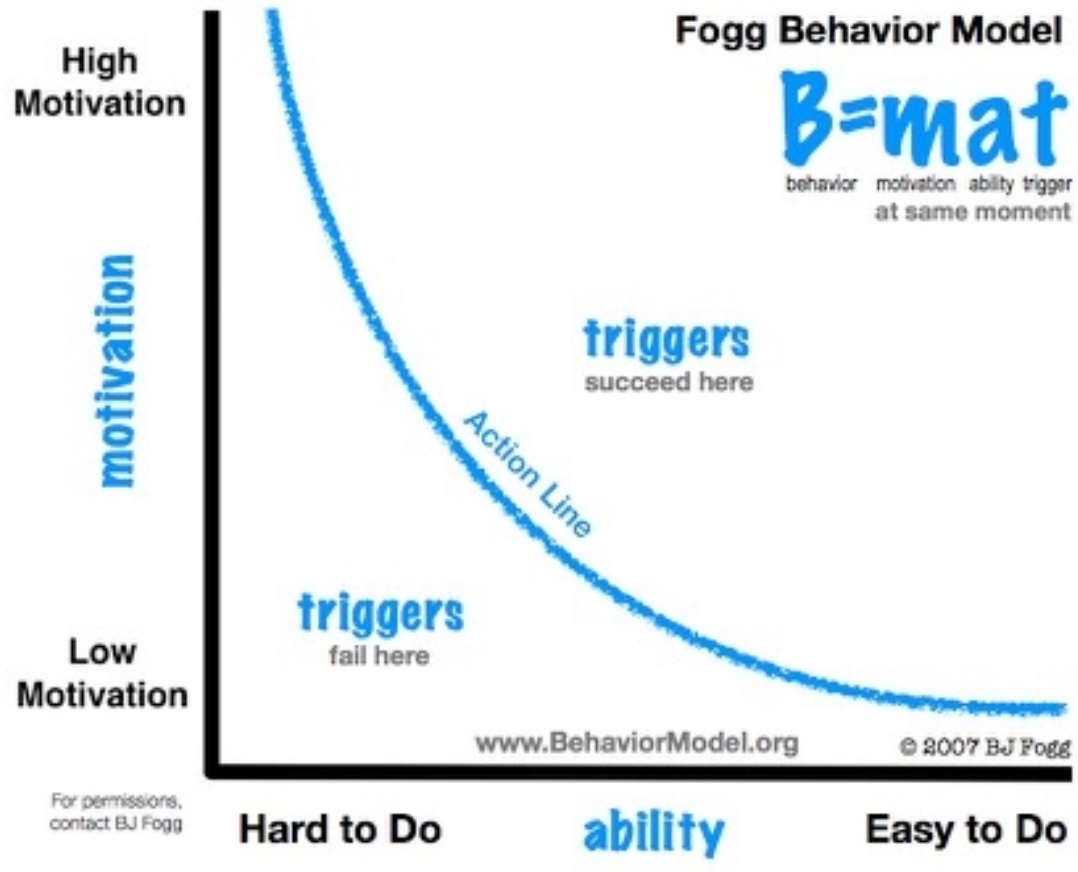
	Q19-Title Categories	#
1.	Awareness & Training – Manager/Director	42
2.	Awareness & Training – Staff	21
3.	Chief Executive Officer (CEO)	3
4.	Chief Financial Officer (CFO)	1
5.	Chief Information Officer (CIO)/Chief Technology Officer (CTO)	24
6.	Chief Information Security Officer (CISO)	50
7.	Chief Operating Officer (COO)/Chief Risk Officer	1
8.	Chief Security Officer (CSO)	6
9.	Communications	14
10.	Consultant	67
11.	Customer Support/Service	12
12.	Engineer	79
13.	Faculty	7
14.	Human Resources	3
15.	InfoSec – Manager/Director	264
16.	InfoSec – Staff	265
17.	IT – Manager/Director	178
18.	IT – Staff	66
19.	Legal/Audit/Compliance	43
20.	Operations/Physical Operations	16
21.	Other	81
22.	Owner	3
23.	President	5
24.	Risk – Manager/Director	21
25.	Risk – Staff	11
26.	Training	13

Q20 - Your Background

Which most closely describes your role before you became involved in security awareness?



BJ Fogg Behavior Model – Curse of Knowledge



Cognitive Overload

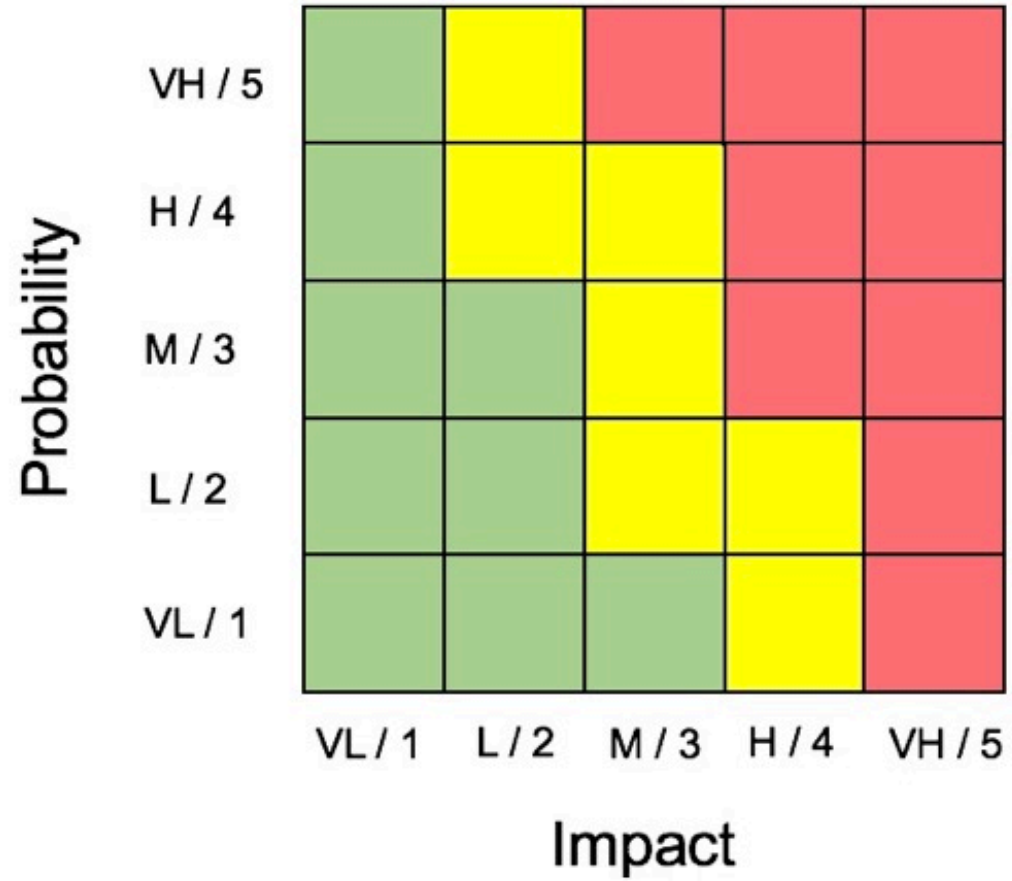
- People can only remember so much
- Security awareness programs can only communicate so much

- First step, communicate as few behaviors as possible.

Dr. Angela Sasse – University College of London

Every behavior has a cost.

Human Risks/Topics	Probability	Impact	Risk Score
Example Risk	Very High	Medium	High
Example Risk	5	3	15
You Are the Shield			
Social Engineering			
Email and Messaging			
Browsing			
Social Networking			
Mobile Device Security			
Passwords			
Malware			
Data Security			
Working Remotely			
Cloud			
Targeted Attacks			
Physical Security			
Creating a Cyber Secure Home			
Hacked			



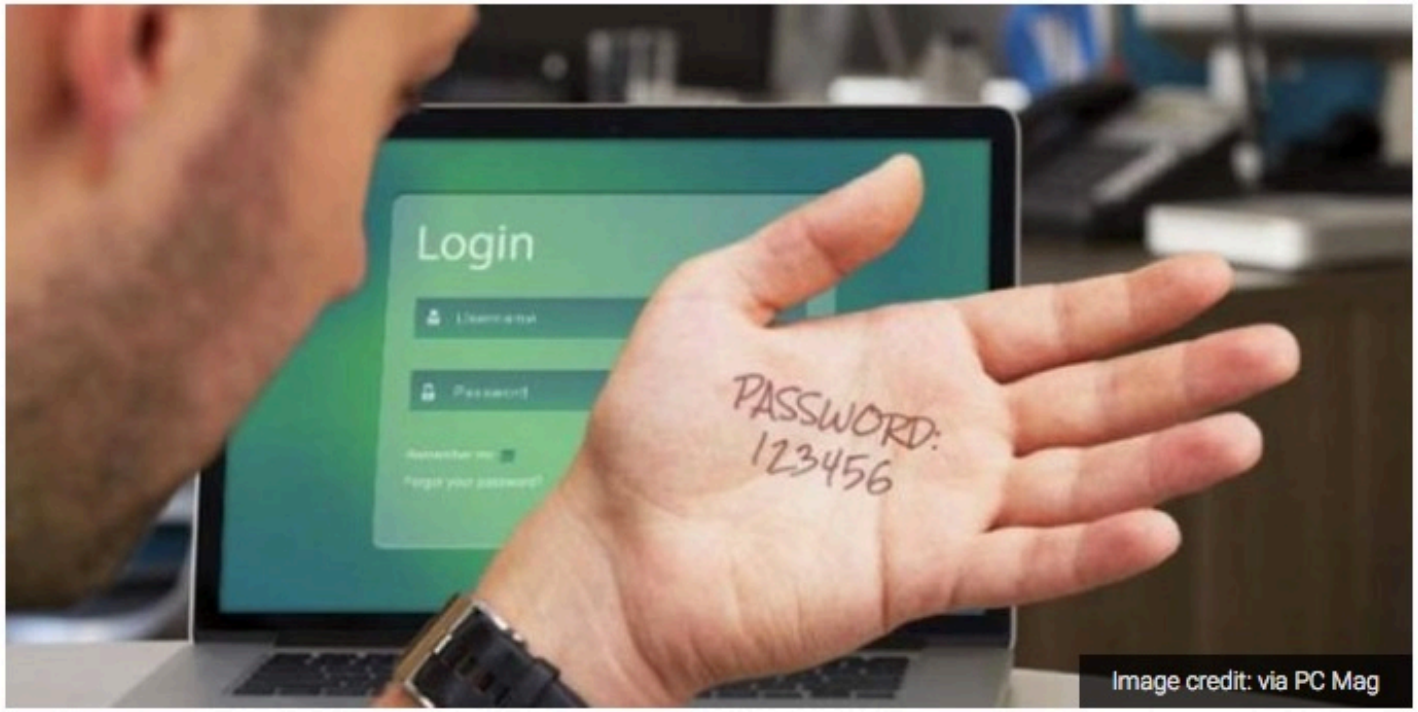
Here Are the 25 Worst Passwords of 2017

New additions to SplashData's list of 2017's worst passwords are letmein, monkey, 123123, hello, freedom, whatever and trustno1.

234 shares

Add to Queue

NEXT ARTICLE ▶



Angela Moscaritolo
Reporter

- 1 Upper Case Letter
- 1 Lower Case Letter
- 1 Symbol
- 1 Number
- Change very 90 days
- Never write it down
- Every password different

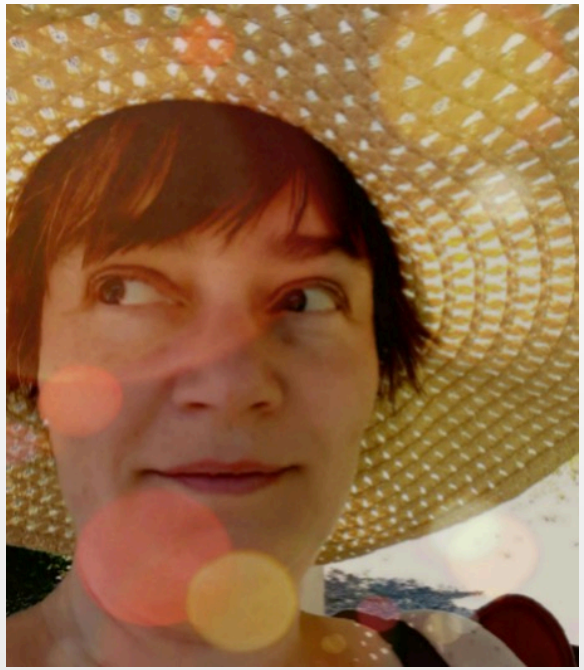
Simplify Passwords

SANS SECURITY AWARENESS

- Passphrases
- Password Managers
- Two-step Verification

Booking.com

It has to be ”Sue” proof.



National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

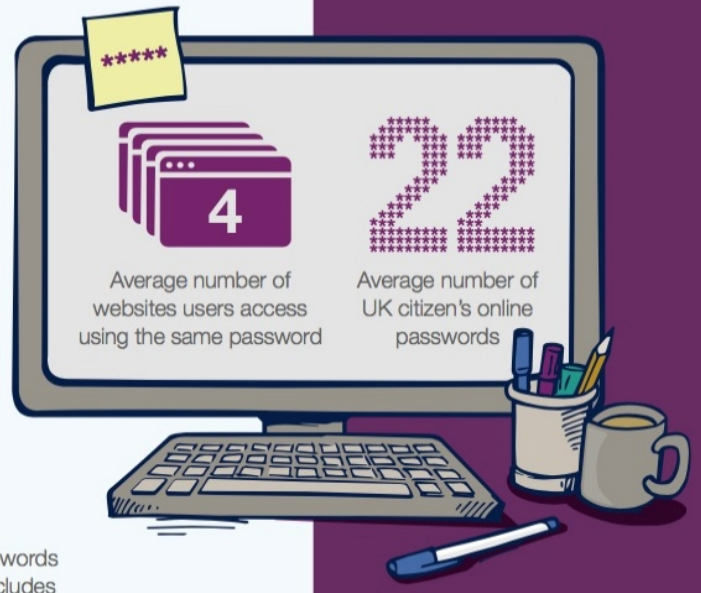
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

What Can We Do?

SANS SECURITY AWARENESS

- Focus on fewest behaviors that have the biggest impact. You should have a good reason for every behavior you teach.
- Simplify those behaviors as much as possible.
- When communicating “Sue proof-it”.

- *If people are not exhibiting a behavior, do not blame them. Ask what the problem is – motivation or ability?*