

The information security crisis: practical steps for your business

Focus on Management - May 2019





Content

2000

The 10 immutable laws of security

2011

Case studies using IR mitigation strategies

2019

Mitigation Strategies



The 10 Immutable Laws of Security.

Scott Culp – Microsoft, 2000

1. If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.

Email



WEAPONS
DIRECTOR 2

W 40

791

2. If a bad guy can alter the operating system on your computer, it's not your computer anymore.



3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

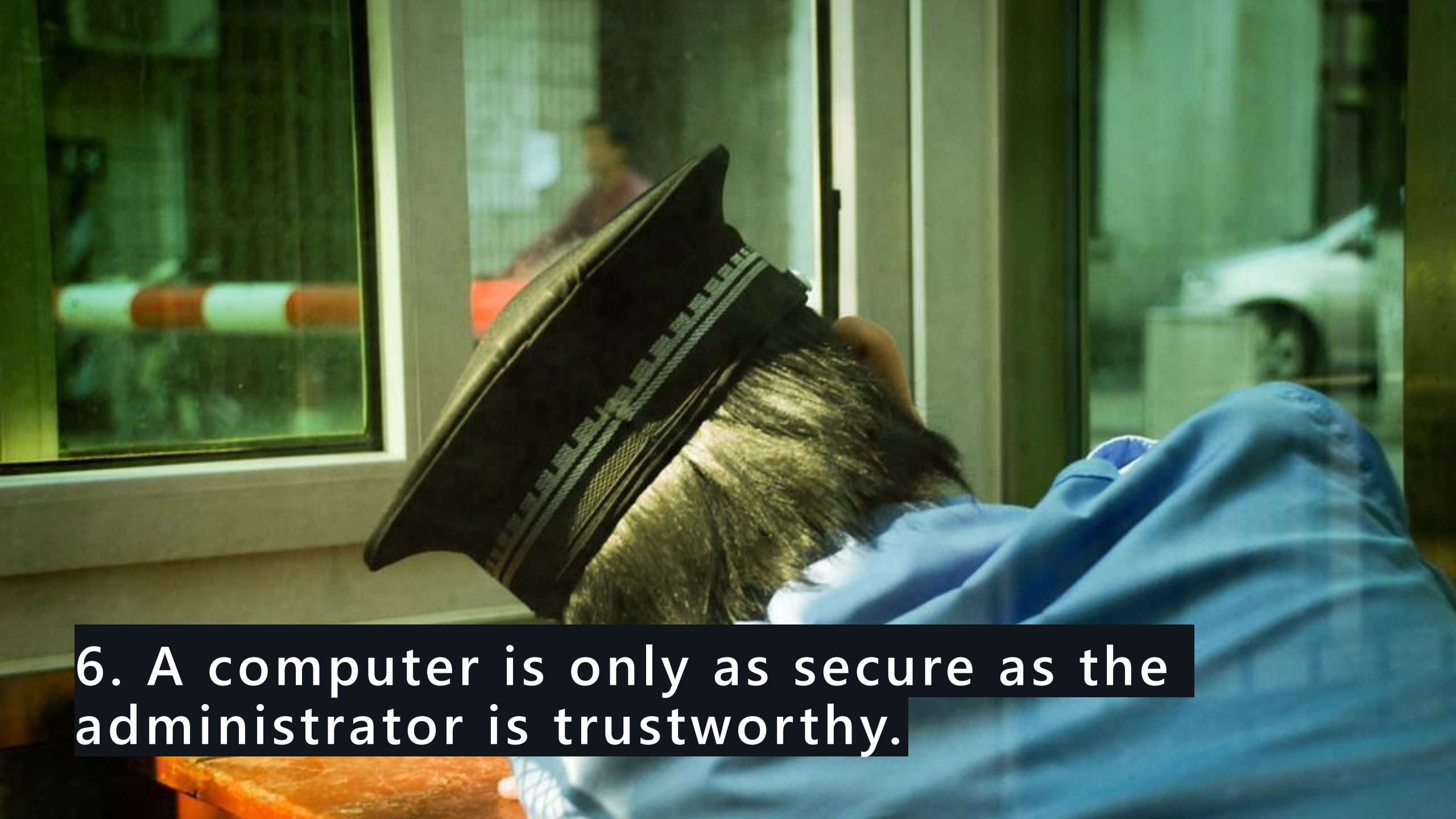
4. If you allow a bad guy to run active content in your website, it's not your website anymore.



O P E N

5. Weak passwords trump strong security.

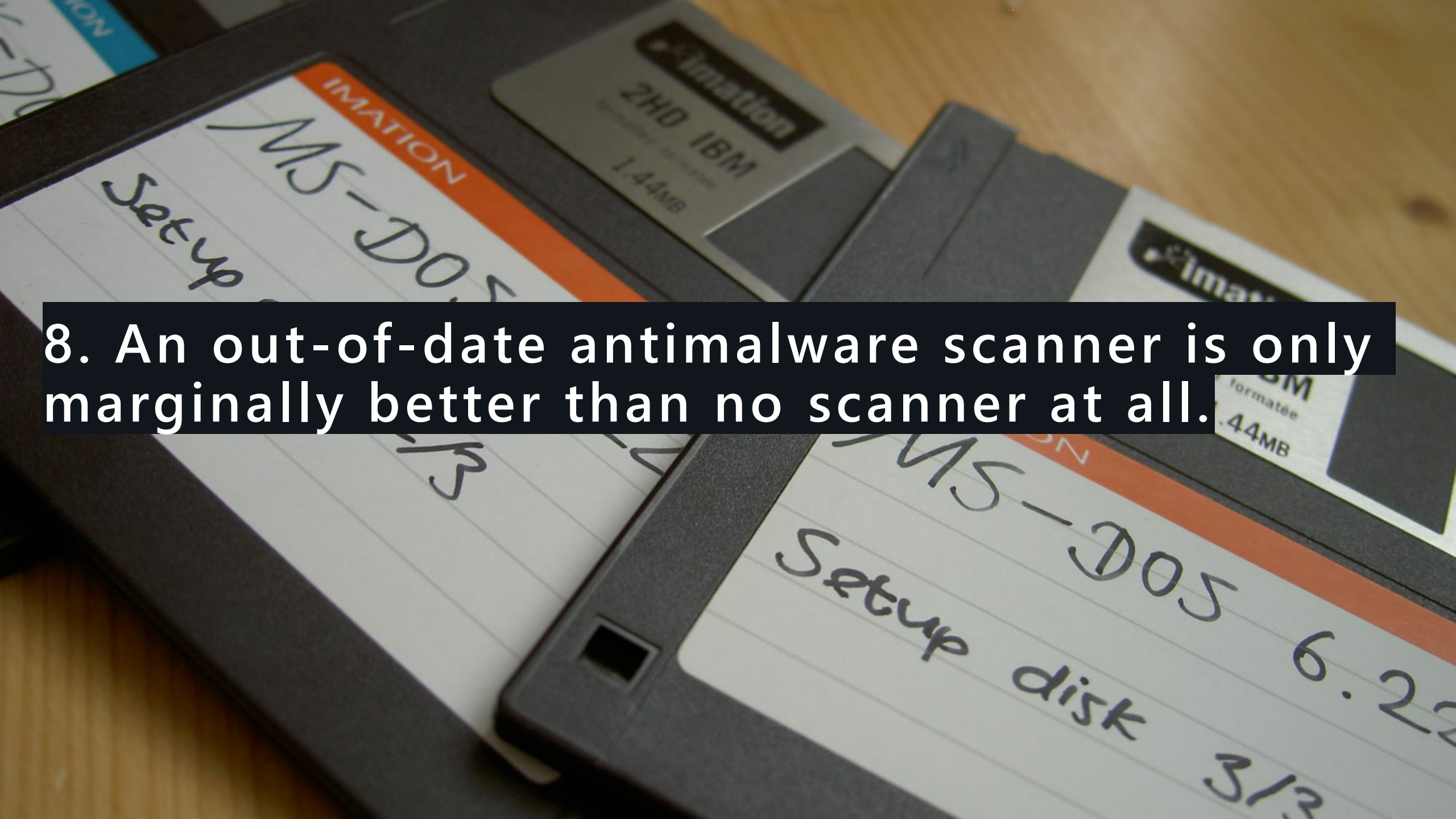
D A T A



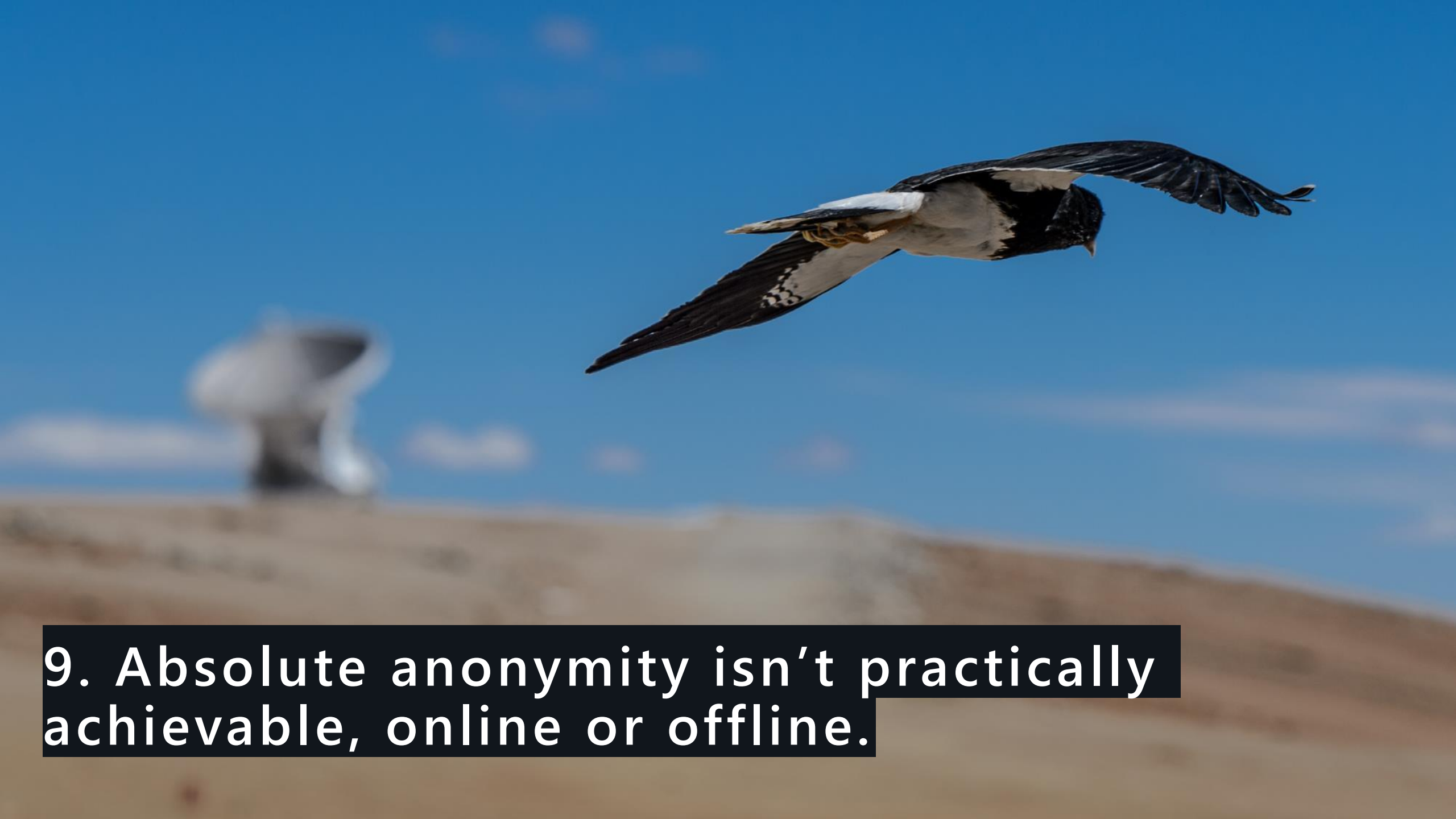
6. A computer is only as secure as the administrator is trustworthy.

7. Encrypted data is only as secure as the decryption key.





8. An out-of-date antimalware scanner is only marginally better than no scanner at all.



9. Absolute anonymity isn't practically achievable, online or offline.

10. Technology is not a panacea.



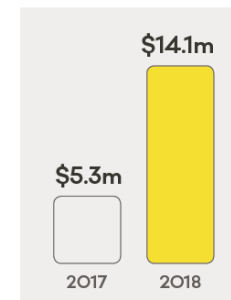
Cybercrime

Financial fraud crimes
Cyberterrorism
Cyberwarfare
Computer as a target
Computer as a tool



Financial loss

18% of reports made to CERT NZ had some form of financial loss with a total value of **\$14 million**.



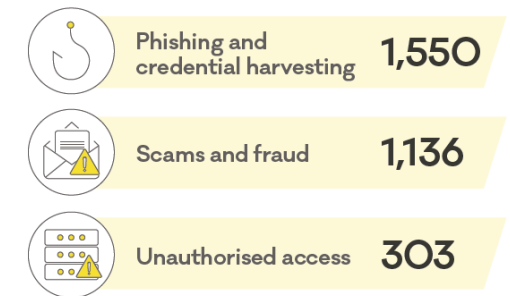
65% of the reports of financial loss **affected individuals**.



Over \$8m of this loss was attributed to scam and fraud reports.

Top incident categories

The **top three incident categories** for 2018 were also the highest in 2017.





Case studies using IR mitigation strategies

Vote – Ransomware or Email Compromise?

Patrick Kral – SANS - Incident Handler's Handbook, 2011

Case Study – Business Email Compromise





Mitigation Strategies

Campbell McKenzie – Incident Response Solutions, 2019

Mitigation Strategies

Back up your data



Using an external hard drive or a cloud-based service, copy your data to another separate location so you can retrieve it if necessary.

Keep your operating system up to date



Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out.

Install antivirus software



Free online antivirus software can be fake. Purchase antivirus software from a reputable company and run it regularly.

Choose unique passwords



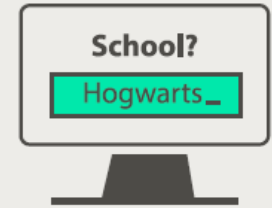
Create unique passwords for each account – that way if an attacker gets hold of one of your passwords, they can't get access to all of your other accounts.

Set up two-factor authentication (2FA)



Choose to get a code sent to another device like your phone when logging in online – it helps stop hackers getting into your accounts.

Use creative recovery answers



Common security answers like your pets name or your school can be easy for an attacker to find out. Choose novel answers that aren't necessarily real.

Be cautious of free WiFi networks



Be careful using free Wifi and hot spots - they are untrusted networks so others could see what you are doing.

Be smart with social media



What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

Don't give out personal info



Legitimate-looking emails are very clever at trying to trick us into giving away personal or financial information. Stop and check if you know who the email is from.

Check bank statements regularly



Keeping an eye on your bank statements could be the first tip-off that someone has accessed your accounts. Ring your bank immediately if you see something suspicious.

Get a regular credit check



An annual credit check will alert you if someone else is using your details to get loans or credit.

To report a cyber security problem, visit
www.cert.govt.nz

Password Managers

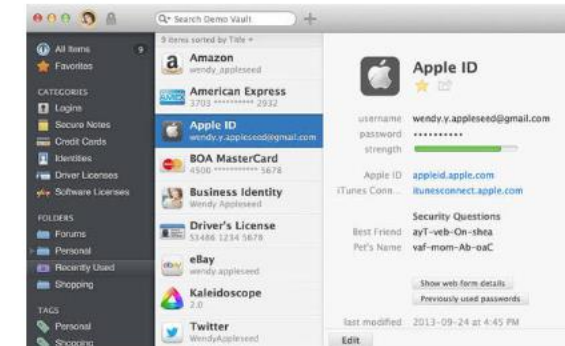
From our test What is a password manager? Strong passwords About our test Broadband Compare Two-factor >

From our test

VIEW ALL

Password manager

1Password



SCORE

SCORE ?

AVERAGE PRICE

\$87

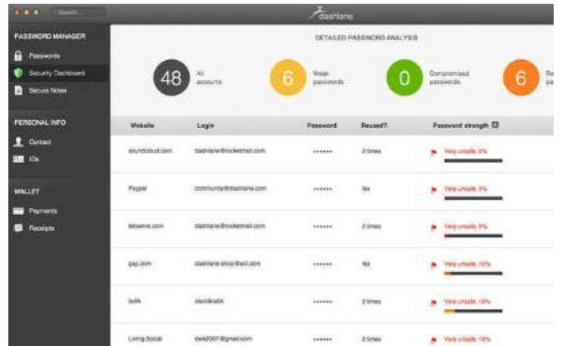
NO MEMBER REVIEWS

Snapshot:

1Password password manager works on Windows, Apple OS X, Android

Password manager

Dashlane



SCORE

SCORE ?

AVERAGE PRICE

\$58

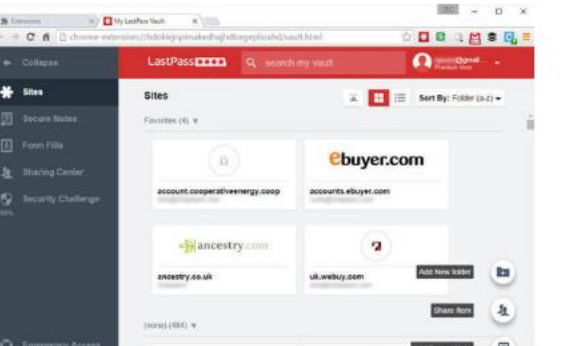
1 MEMBER REVIEW

Snapshot:

Dashlane password manager works on Windows, Apple OS X, Android

Password manager

LastPass Premium



SCORE

SCORE ?

AVERAGE PRICE

\$17

3 MEMBER REVIEWS

Snapshot:

LastPass Premium password manager works on Windows, Apple OS X,

INCIDENT RESPONSE SOLUTIONS

We help you Prepare, Respond and Recover
from Forensic and Cyber Incidents

Campbell McKenzie

+64 21 779 310

campbell@incidentresponse.co.nz

<https://incidentresponse.co.nz>

