



How Safe is Your Data?

7 Steps of Hacking - 25th April 2018

Learning Objectives

You will:

- **Understand the steps that hackers use to infiltrate companies and employees to steal their data**
- **Understand how hackers identify a target company or employee**
- **Understand why we all have a responsibility to keep our data secure.**
- **Understand how targeted electronic equipment can be used to infiltrate companies or employees.**
- **Understand simple defences to protect yourself.**

Recent Headlines

Password guru Bill Blur regrets past password advice in interview with Wall Street Journal August 2018

MyFitnessPal Suffers Data Breach. 150million users details stolen.

Cyrtojacking attacks surge 1,200% as UK Bitcoin value grows

Rampant Ransomware encrypts files, holding business hostage

Hackers could take over electricity grid through solar panel gear

Equifax exposes personal data of 143 million consumers

Cyber criminals stealing reward points for luxury holidays

Data breaches following Cyber attacks in 2016 was in excess of 3.1 billion records leaked

North Korea poses a greater Cyber Attack threat than Russia

The ICO (Data Watchdog) has "huge concerns" over Uber data breach

Does anyone know the global cost of cybercrime to the Global Economy?

It is estimated to cost the global
economy more than

**£338 billion every year
and Projected to reach
£1.5 trillion by 2019**

McAfee, Net Losses: Estimating the Global Cost of
Cybercrime (June 2014) & Steve Morgan
Forbes Tech column

What is an Ethical Hacker?

An ethical hacker is a **computer and network expert**, employed to attack a system on behalf of its owners, seeking vulnerabilities a malicious hacker could exploit.

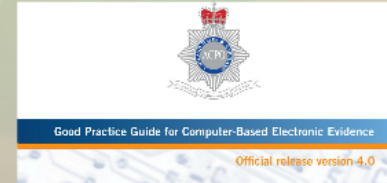
**What is the difference
between:**

**an amateur hacker
&
a professional hacker?**

Our Expertise



Source: Observer 29th October 1995



http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf

Certifications



the Observer 29 October 1995

RAF covertly taps mobile phones

'Special dispensation' by DTI threatens privacy

Peter Beaumont
Defence Correspondent

A SECRETIVE Royal Air Force unit dedicated to gathering and protecting electronic intelligence is monitoring calls on Britain's public mobile telephone networks — despite acknowledging the risk of 'accidentally' eavesdropping on private conversations.

The Observer has established that 591 Signals Unit, based at RAF Digby in Lincolnshire, has been monitoring mobile calls since at least the middle of this year, after the

forming 'defensive monitoring' of RAF radio frequencies and their own telephone and fax systems to spot people discussing classified material on open lines or frequencies.

Until last year the RAF was prevented from monitoring mobile calls under the 1990 Interception of Communications Act. Now, however, the unit has been given special permission by the Department of Trade and Industry to monitor mobile telephone traffic.

The new exception to the Act follows concern over the increased use of portable telephones by RAF personnel and

about telephone monitoring across the three armed services.

Labour MP Chris Mullin said: 'There is obvious scope for abuse. Like most people, I am very surprised that the RAF should be able to listen in to open public networks and I believe we should be told more about this.'

The issue is to be raised by Labour's Shadow Defence Secretary, David Clark, who is to ask which other mobile phone networks are being monitored by the armed forces.

A spokesman for the RAF conceded that the law had

Source: Observer 29th October 1995

Certifications





Good Practice Guide for Computer-Based Electronic Evidence

Official release version 4.0

[http://www.7safe.com/electronic_evidence/
ACPO_guidelines_computer_evidence_v4_web.pdf](http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf)

Who is at risk?

Chip and PIN terminal users

Businesses with competitors

Large organisations

Anyone with a computer!

7 Steps to Hacking

Step 1 Information Discovery

Research the target

Dumpster diving Social Engineering
Real World Gathering Companies House
Current clients Company Website
The Internet! Company Testimonials

Step 3 Vulnerability Assessment

The information gathered from steps 1 & 2 helps the hacker decide on the best method of attack

This is determined by the hacker

Selecting the path of least resistance

Step 2 Target Scanning

Identify potential entry points

Physical access or virtual?

Determines a hacker's chosen method of attack

Virtual Access
The hacker uses a remote access tool to gain access to the target system.

Physical Access
The hacker gains access to the target system by physically entering the premises.

Step 4 Exploiting the weakness

Virtual access example

The Trojan Email

Physical access example

The Trojan Keyboard

Step 5 Privilege Escalation

Establish self as a trusted user

Gain administrative privileges

All computers, printers and devices are now exposed to the hacker

This is known as "owning the network"

Step 7 Covering Tracks

Hide the evidence of being hacked

Retain anonymity, ranging in severity
Changing file metadata and permissions,
Corrupting files, folders and Master Boot
Records

Back out of the computer or network

Step 6 Retaining Access

Owning the network allows you to:

Open other routes/backdoors into the network

Complete the required task for the original hack

Step 1

Information Discovery

Research the target

Dumpster diving

Social Engineering

Real World Gathering

Companies House

Current clients

Company Website

The Internet!

Company Testimonials

Step 2

Target Scanning

Identify potential entry points

Physical access or virtual?

Determines a hacker's chosen method of attack

Virtual Access

Email servers
Standard router credentials
Insecure wireless networks
Remote web workplace
Outlook web access
Targeted electronic equipment
Remote Desktop

Physical Access

Disgruntled employee or former employee
Lax security and procedures
Third party contractors, e.g. agency staff
Targeted electronic equipment

Virtual Access

Email servers

Standard router credentials

Insecure wireless networks

Remote web workplace

Outlook web access

Targeted electronic equipment

Remote Desktop

Physical Access

Disgruntled employee or former employee

Lax security and procedures

Third party contractors, e.g. agency staff

Targeted electronic equipment

Step 2

Target Scanning

Identify potential entry points

Physical access or virtual?

Determines a hacker's chosen method of attack

Virtual Access

Email servers
Standard router credentials
Insecure wireless networks
Remote web workplace
Outlook web access
Targeted electronic equipment
Remote Desktop

Physical Access

Disgruntled employee or former employee
Lax security and procedures
Third party contractors, e.g. agency staff
Targeted electronic equipment

Step 3

Vulnerability Assessment

The information gathered from steps 1 & 2 helps the hacker decide on the best method of attack

This is determined by the hacker

Selecting the path of least resistance

Step 4

Exploiting the weakness

**Virtual access
example**

The Trojan Email

**Physical access
example**

The Trojan Keyboard

Step 5 Privilege Escalation

Establish self as a trusted user

Gain administrative privileges

All computers, printers and devices are
now exposed to the hacker

This is know as "owning the network"

Step 7 Covering Tracks

Hide the evidence of being hacked

Retain anonymity, ranging in severity
Changing file metadata and permissions,
Corrupting files, folders and Master Boot
Records

Back out of the computer or network

Step 6 Retaining Access

Owning the network allows you to:

Open other routes/backdoors into the network

Complete the required task for the
original hack

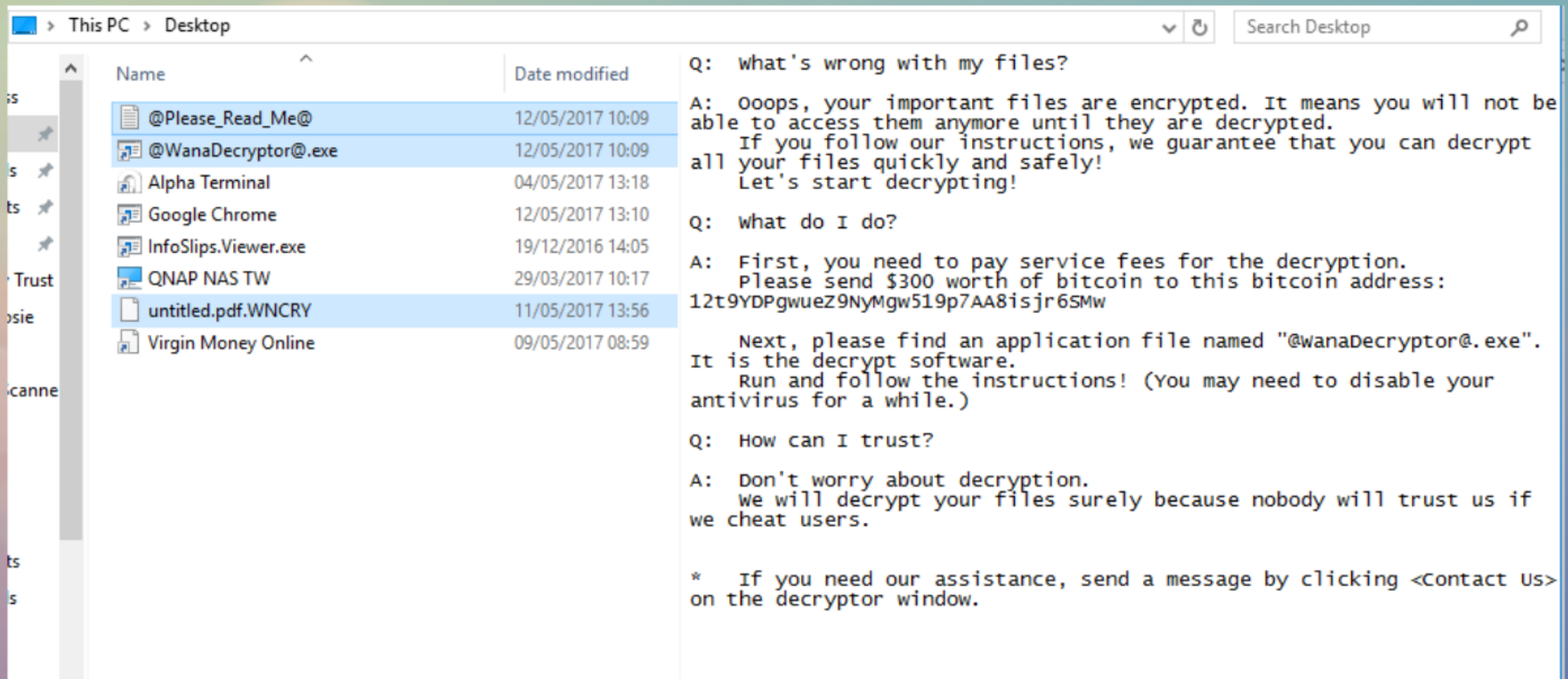
How much does it cost to become James Bond?

James Bond's Budget

| | |
|--------------------------------|-------------|
| 'Spy sunglasses | £225 |
| key-fob recording device | £175 |
| Nokia charger recording device | £200 |
| Keystroke logger | £35 |
| 'Spy watch' | £100 |
| Bugged phone | £200 |
| Total | £935 |



Wanacrypt Ransomware Example



The screenshot shows a Windows File Explorer window titled 'This PC > Desktop'. The left pane shows a list of files and folders on the desktop. The right pane displays the contents of the selected file, '@Please_Read_Me@', which is a ransomware message. The message is written in a monospaced font and contains the following text:

| Name | Date modified |
|----------------------|------------------|
| @Please_Read_Me@ | 12/05/2017 10:09 |
| @WanaDecryptor@.exe | 12/05/2017 10:09 |
| Alpha Terminal | 04/05/2017 13:18 |
| Google Chrome | 12/05/2017 13:10 |
| InfoSlips.Viewer.exe | 19/12/2016 14:05 |
| QNAP NAS TW | 29/03/2017 10:17 |
| untitled.pdf.WNCRY | 11/05/2017 13:56 |
| Virgin Money Online | 09/05/2017 08:59 |

Q: what's wrong with my files?
A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
Let's start decrypting!

Q: what do I do?
A: First, you need to pay service fees for the decryption.
Please send \$300 worth of bitcoin to this bitcoin address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Next, please find an application file named "@wanaDecryptor@.exe". It is the decrypt software.
Run and follow the instructions! (You may need to disable your antivirus for a while.)

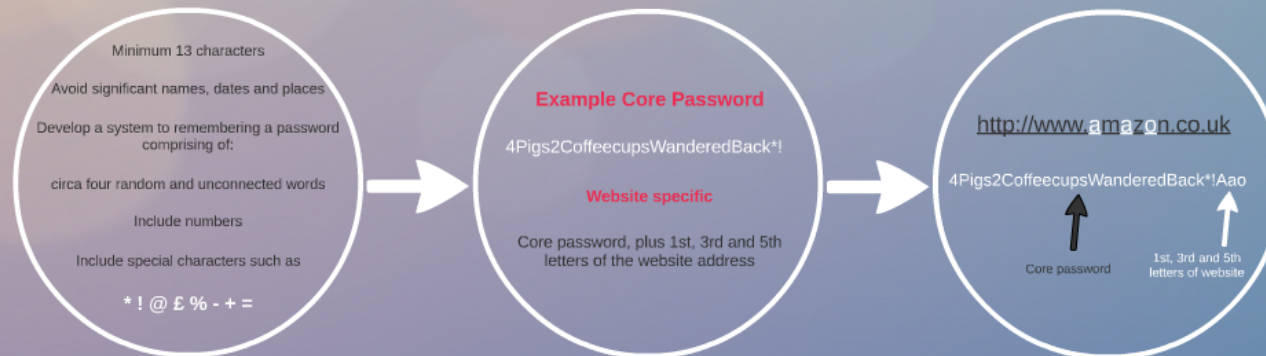
Q: How can I trust?
A: Don't worry about decryption.
We will decrypt your files surely because nobody will trust us if we cheat users.

* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.

Simple rules for a first line of defence

- Educate your employees about the risks
- Install all security updates when released
- Consider information you place on the web
- Ensure all internal firewalls are always on
- Introduce clear desk policies
- Vet third-party contractors
- Get Cyber Crime Insurance
- Lock unattended computers
- Check user rights regularly
- Avoid writing passwords down...

Password Policies



Minimum 13 characters

Avoid significant names, dates and places

Develop a system to remembering a password
comprising of:

circa four random and unconnected words

Include numbers

Include special characters such as

* ! @ £ % - + =

Example Core Password

4Pigs2CoffeecupsWanderedBack*!

Website specific

Core password, plus 1st, 3rd and 5th letters of the website address

<http://www.amazon.co.uk>

4Pigs2CoffeecupsWanderedBack*!Aao



Core password



1st, 3rd and 5th
letters of website

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.



Manual Guessing

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



Social Engineering

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



Stealing Passwords

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

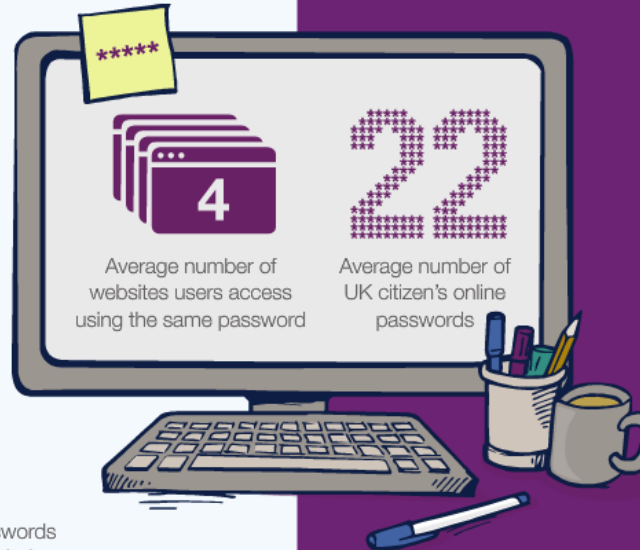
Shoulder Surfing

Observing someone typing their password.



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



Summary

The higher up the tree you are,
the safer you will become



To beat a hacker...
you need to think like one!

Any Questions?

SteveMac
MEDIA

Steve McLaughlin (Director)

Steve Mac Media Limited
Marne House
24 Mount Ephraim Road
Tunbridge Wells
Kent TN1 1ED

Mobile: 07919 406224
www.stevemacmedia.co.uk
steve@stevemacmedia.co.uk

