



VerticalStructure

Cyber Security

The Community & Voluntary Sector

Simon Whittaker

Cyber Security Director - Vertical Structure Ltd

Prepare, Protect, Persist ®



Prepare

We help you and your partners to understand how to identify and resolve potential security issues at the earliest stages with hands on 'hack yourself first', threat modelling and GDPR compliance workshops as well as security training for non-technical colleagues.

Protect

Using automated and manual penetration testing techniques, we provide a comprehensive security report for your Web and mobile applications, including API testing, and networks. The report highlights potential issues and their resolutions.

Persist

We ensure that your organisation benefits from continual improvements in security levels through information assurance processes, auditing and certification including ISO27001:2013 and Cyber Essentials.

Why is the sector being targeted?



UK charities hold:

- Funds
- Personal
- Financial and commercial data
- Other information that is of interest or monetary value to a range of cyber criminals and other groups.

<https://www.ncsc.gov.uk/collection/charity>

**NI Cyber exists to promote the expertise of >35 companies from NI,
identifying opportunities for business and national/international collaboration,
and promoting career opportunities in cyber security.**



NI CYBER
Northern Ireland Cyber Security Cluster



ANOMALI



Deloitte.



kainos®



Novosco

proofpoint



RAPID7



Titan
IC

ULESKA



Speakers



Simon Whittaker – Cyber Security Director - Vertical Structure

The majority of my work involves working with companies to perform penetration & security testing, test and improve secure coding practices and provide security consultancy to companies that are keen to improve their processes & procedures.

simon.whittaker@verticalstructure.com

Why is the sector being targeted?



Charities are subject to the same cyber vulnerabilities as other organisations and businesses that conduct financial transactions, and rely on electronically held data or information to conduct day-to-day operations.

Why is the sector being targeted?



The outward facing nature of charities and a culture of trust in the sector makes them particularly vulnerable to criminality.



The Governance Jigsaw – The Essential Trustee (CC3)



It's about knowing:

- what your charity can and can't do within its purposes
- how your charity is fulfilling its purposes and benefiting the public
- what difference your charity is really making

It's about being:

- familiar with your governing document
- up to date with filing accounts, returns and any changes to your charity's registration details
- aware of other laws that apply to your charity

It's not about being:

- an expert - but you do need to take reasonable steps to find out

It's about:

- making balanced, informed decisions
- recognising & dealing with conflicts of interest
- ensuring trustee benefits are allowed
- being prepared to question and challenge
- accepting majority decisions

It's not about:

- preserving the charity for its own sake
- serving personal interests

It's about:

- managing risks, protecting assets (reputation) and people
- getting the resources your charity needs
- having and following appropriate controls and procedures
- dealing with land and buildings
- responsibility for, and to staff and volunteers

It's about:

- using your skills and experience
- deciding when you need advice
- preparing for meetings
- getting the information you need (financial, management)
- being prepared in case something does go wrong

It's about:

- meeting legal accounting and reporting requirements
- being able to show that your charity complies with the law and is effective
- being accountable to members and others with an interest in the charity
- ensuring that staff and volunteers are accountable to the board
- welcoming accountability as an opportunity not a burden

Some Findings



- UK charities hold funds, personal, financial and commercial data and other information that is of interest or monetary value to a range of cyber criminals and other groups.
- The type and amount of information held varies according to an individual charity's size, objectives, structure and contacts.
- Charities are subject to the same cyber vulnerabilities as other organisations and businesses that conduct financial transactions, and rely on electronically held data or information to conduct day-to-day operations.
- Thirty charities interviewed for a recent government-commissioned report had collectively experienced a range of cyber breaches in the last two years including viruses, phishing emails, ransomware attacks, identity theft, website takedowns and variants of online financial fraud.
- The breaches resulted in loss of funds, data and website control. Although based on a very small dataset, the findings suggest that malicious cyber activity against the charity sector is varied and enduring.

<https://www.ncsc.gov.uk/files/Cyber%20threat%20assessment%20-%20UK%20charity%20sector.pdf>

Cyber Security Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/charity.



Backing up your data

Take **regular** backups of your important data, and **test** they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.



Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.



Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.



Switch on PIN/password protection/fingerprint recognition for mobile devices.



Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.



Keep your devices (and all installed apps) **up to date**, using the 'automatically update' option if available.



When sending sensitive data, don't connect to public Wi-Fi hotspots - use **3G or 4G connections** (including tethering and wireless dongles) or use **VPNs**.



Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.



Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.



Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.



Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.



Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



Ensure staff don't browse the web or check emails from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.



Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).



Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.



Make sure all laptops, MACs and PCs use encryption products that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.



Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.



Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *password*).



Do not enforce regular password changes; they only need to be changed when you suspect a compromise.



Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.



Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.



Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

The Assessment



Cyber threat assessment: UK charity sector

February 2018



<https://www.ncsc.gov.uk/files/Cyber%20threat%20assessment%20-%20UK%20charity%20sector.pdf>

Where are we?



Advice from the experts



National Cyber
Security Centre

a part of GCHQ

<https://www.ncsc.gov.uk/guidance/home-working>

Passwords



- Set strong and long passwords for your users
- 2FA wherever possible
- Consider admin users separately



Your team may be confused

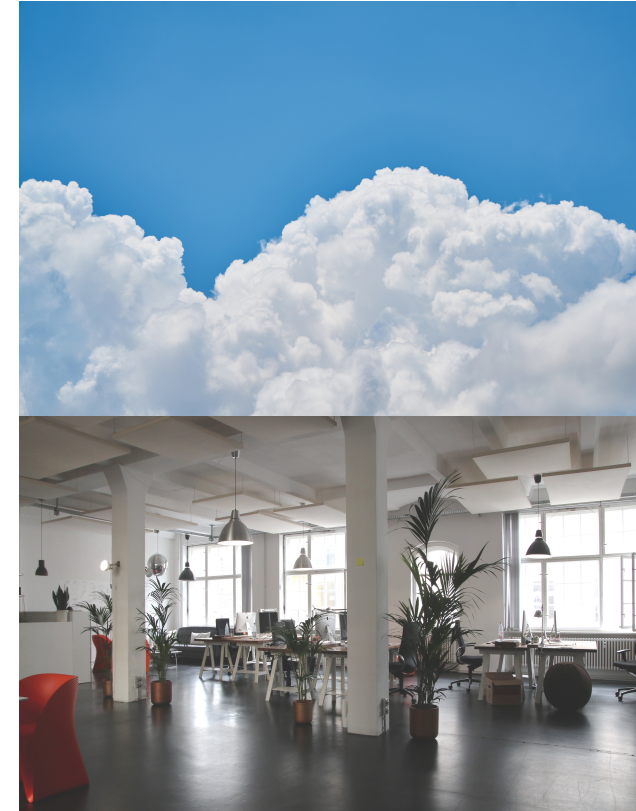


- Make software easily accessible
- Write howto guides for **everything**
- What hardware should they use?
- Microsoft Tech Support Calls

Don't leave the doors unlocked



- Secure your cloud
- Secure your office
- Secure your connectivity



Devices



- Bring Your Own?
- Encryption
- Remote Wipe
- Loss of Control of data
- Anti-Malware

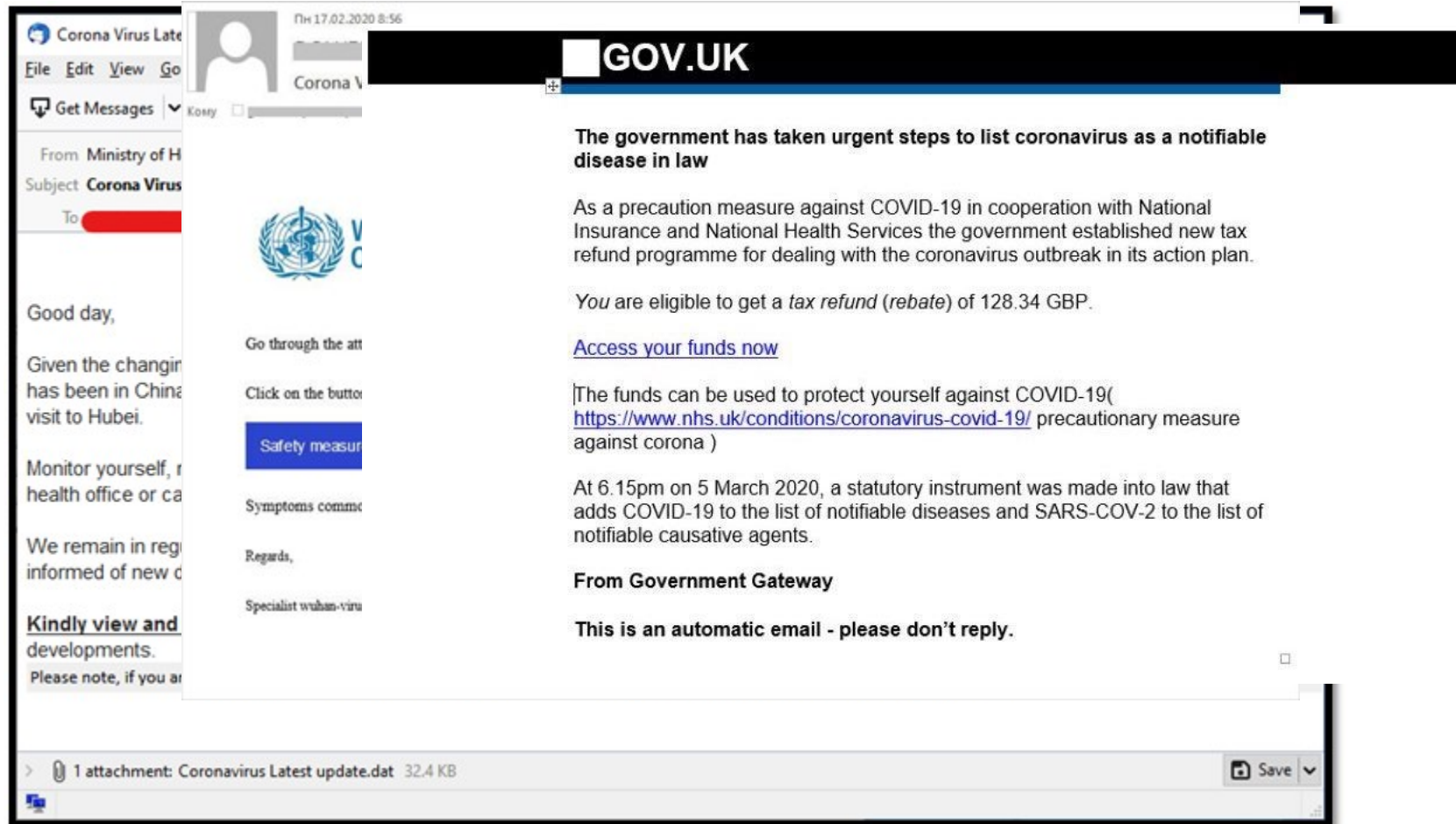
Devices



- Free Wifi usage
- USB drives
- Backups
- Software updates



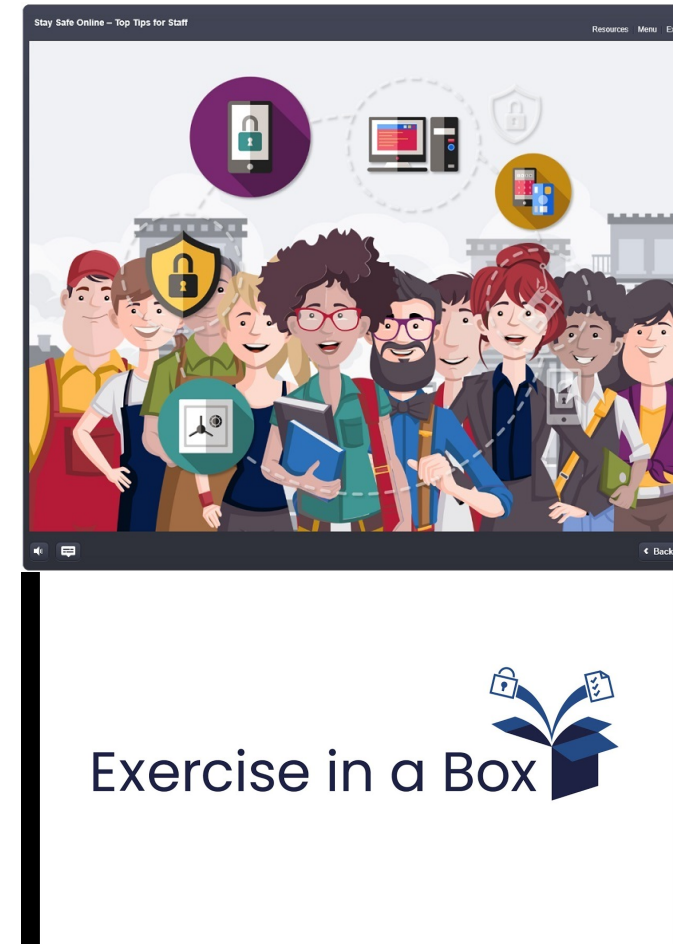
The scamming doesn't stop



Provide Training & Guidance



- NCSC training for all
- Practice your incident response before it happens



Passwords

Have you been pwned?



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

simon.whittaker@verticalstructure.com **pwned?**

Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

simon@verticalstructure.com **pwned?**

Oh no — pwned!
Pwned on 7 breached sites and found no pastes (subscribe to search sensitive breaches)

www.haveibeenpwned.com

Password Policies



Users are generally told to remember passwords, and to not share them, re-use them, or write them down. But the typical user has dozens of passwords to remember – not just yours. Regular password changing harms rather than improves security, so avoid placing this burden on users. However, users must change their passwords on indication or suspicion of compromise.

Gov.uk advice on passwords

<https://www.ncsc.gov.uk/guidance/password-guidance-summary-how-protect-against-password-guessing-attacks>

Password Guidance



1. Change all default passwords
2. Help users cope with password overload
3. Understand the limitations of user-generated passwords
4. Understand the limitations of machine-generated passwords
5. Prioritise administrator and remote user accounts
6. Use account lockout and protective monitoring
7. Don't store passwords as plain text



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.

...and how to improve your system security

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



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

IT infrastructure can be searched for electronically stored password information.



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

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



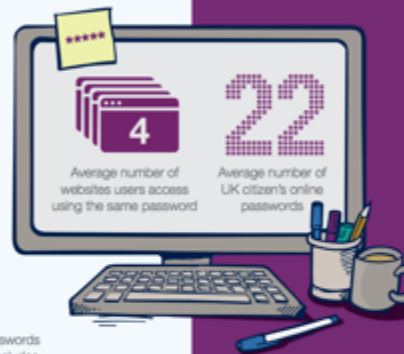
Observing someone typing their password.



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



An installed keylogger intercepts passwords as they are typed.



- 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.

- Put technical defenses 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



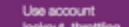
- Prioritise administrator and remote user accounts



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



For more information go to www.ncsc.gov.uk @ncsc



Password availability



GitHub, Inc. [US] | <https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials>

g to... Pull requests Issues Marketplace Explore

danielmiessler / SecLists Watch 1,317 Unstar 15,542

Code Issues 6 Pull requests 1 Projects 0 Wiki Insights

Branch: master SecLists / Passwords / Common-Credentials / Create new file Upload files Find

g0tm1k Quick rename Latest commit b61

--

| | |
|--------------------------------------|---|
| 10-million-password-list-top-100.... | Renamed folders to be the 'full' names |
| 10-million-password-list-top-100... | Renamed folders to be the 'full' names |
| 10-million-password-list-top-100... | Renamed folders to be the 'full' names |
| 10-million-password-list-top-100... | Renamed folders to be the 'full' names |
| 10-million-password-list-top-100... | Fixed 10-million-password-list-top-1000000.txt with control character (...) |
| 10-million-password-list-top-500... | Renamed folders to be the 'full' names |
| 10k-most-common.txt | Renamed folders to be the 'full' names |
| 500-worst-passwords.txt | Renamed folders to be the 'full' names |
| SplashData-2014.txt | Renamed folders to be the 'full' names |
| SplashData-2015-1.txt | Renamed folders to be the 'full' names |
| SplashData-2015-2.txt | Renamed folders to be the 'full' names |

danielmiessler / SecLists Watch 1,317 Unstar 15,542 Fork 5,569

Code Issues 6 Pull requests 1 Projects 0 Wiki Insights

Branch: master SecLists / Passwords / Common-Credentials / 10-million-password-list-top-100.txt Find file Copy path

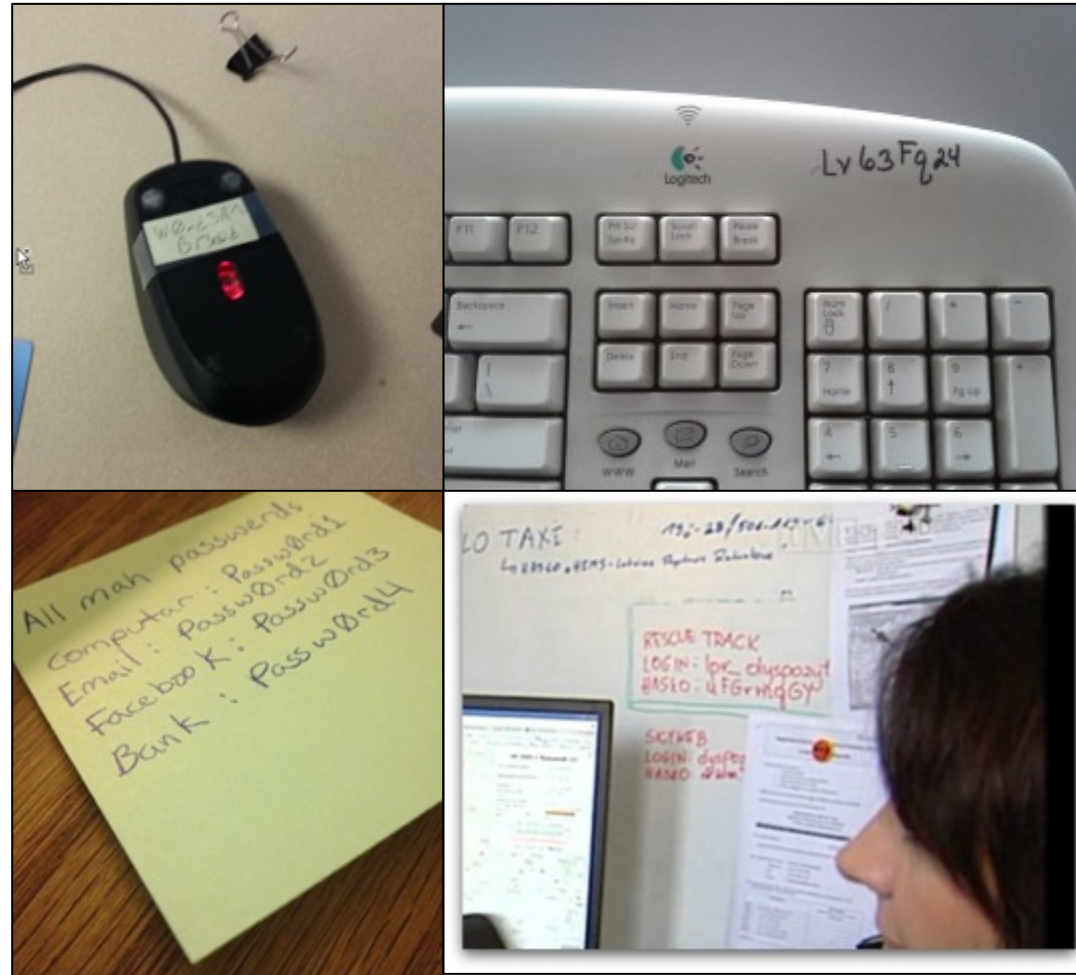
g0tm1k Renamed folders to be the 'full' names 4f84b3c on 5 Mar

1 contributor

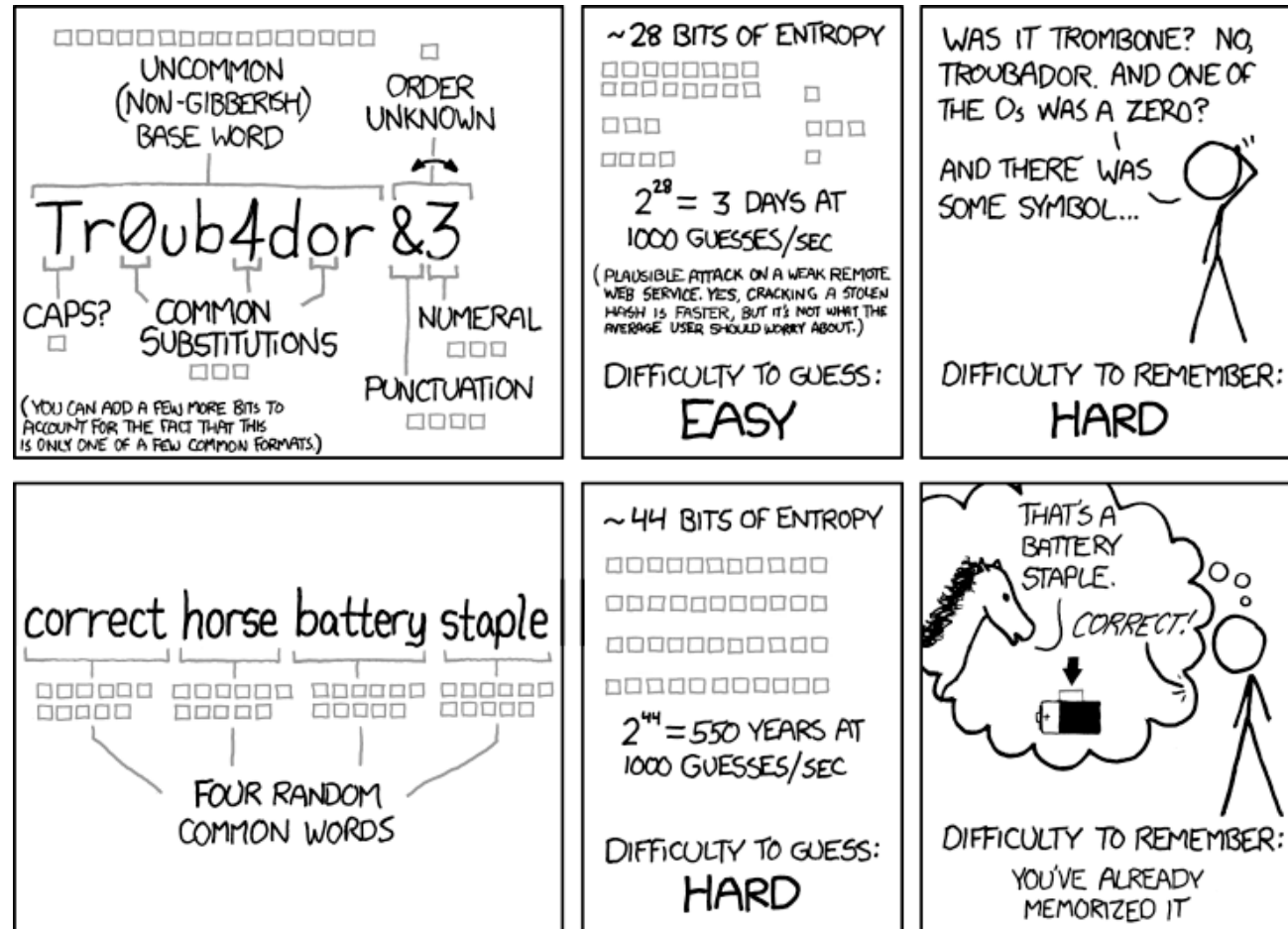
101 Lines (100 sloc) 744 Bytes Raw Blame History

```
1 123456
2 password
3 12345678
4 qwerty
5 123456789
6 12345
7 1234
8 111111
9 1234567
10 dragon
11 123123
12 baseball
13 abc123
14 football
15 monkey
16 letmein
17 666666
18 shadow
19 master
20 666666
21 qwertyuiop
22 123321
23 mustang
24 1234567890
25 michael
```

Some thoughts on passwords



Some thoughts on passwords



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: <https://xkcd.com/936/>

© Vertical Structure Ltd where applicable
simon.whittaker@verticalstructure.com

Password Managers



LastPass...



KeePass

What is better than a password?



https://commons.wikimedia.org/wiki/File:CryptoCard_two_factor.jpg

Listen to your users



Amy has her passwords written on a post-it note under her keyboard.

Brian keeps backups of important data on his personal pen drive.

Claire let David use her account – just for five minutes – while she went to make a cup of tea.

People break the rules because they need to get the job done.

<https://www.ncsc.gov.uk/blog-post/security-breaches-communication-what-are-your-users-telling-you>

Backups



Phishing



Toolkit for boards





National Cyber Security Centre
a part of GCHQ

Cyber Security Toolkit for Boards

Cyber security is central to an organisation's health and resilience, which means it's the Board's responsibility.

Managing cyber security is a continuous, iterative process, but broadly speaking there are three overlapping components, summarised below.

For these steps to be effective, you'll also need to get the environment right.

For more information, please visit www.ncsc.gov.uk/collection/board-toolkit




1

Gather information

Get the information you need to make well-informed decisions about the risks you face.

Establish what is important to you.
Find out what your estate looks like.
Identify your vulnerabilities.
Identify what might be of value to an attacker.
Identify who might target you, and how they would do it.




2

Prioritise your risks

Use this information to understand and prioritise your risks.

Good risk management should go beyond just compliance.

Integrate cyber security into organisational risk management processes.



3

Take steps to manage your risks

Take steps to manage those risks.

Make arrangements with any suppliers, providers or partners to mitigate the risks posed by supply chain attacks.

Implement suitable defences, focused on mitigating your risks.


Have plans in place for when things go wrong.


Getting the environment right


Embedding cyber security in your organisation
Cyber security is not just 'good IT' - it must enable an organisation's digital activity to flourish.

Developing a positive cyber security culture
Board members should lead by example to help promote a healthy cyber security culture.

Growing cyber security expertise
As the demand for cyber security professionals grows, you need to plan ahead to ensure your organisation can draw upon the expertise you need.

 @ncsc

 National Cyber Security Centre

 www.ncsc.gov.uk

© Crown Copyright 2019

<https://www.ncsc.gov.uk/collection/board-toolkit>



Cyber Insurance – basic advice



IASME Cyber Insurance with CyberEssentials

Don't have 2 policies!

Cyber Insurance – a bit more



Should cover the first-party and third-party financial and reputational costs if data or electronic systems have been lost, damaged, stolen or corrupted.

Should include the cost of investigating a cybercrime, recovering data lost in a security breach and the restoration of computer systems, loss of income incurred by a business shutdown, reputation management, extortion payments demanded by hackers, and notification costs, in the case you are required to notify third parties affected.

Third-party coverages (that result from claims against you) include damages and settlements, and the cost of legally defending yourself against claims of a GDPR breach.

What can I do right now?



Passwords

- Get a password manager
- Use 2 factor authentication

Malware

- Buy an antivirus

Train your users

- NCSC training
- CyberEssentials

Takeaways



1. NCSC Guide for Charities
 - <https://www.ncsc.gov.uk/collection/charity>
2. Cyber Operations Cost
 - <https://www.recordedfuture.com/cyber-operations-cost/>
3. Data Breach List
 - <https://www.privacyrights.org/data-breaches>
4. Taking the offensive
 - <http://www.globalservices.bt.com/content/dam/globalservices/documents/whitepapers/taking-the-offensive.pdf>
5. NCSC small business advice
 - <https://www.ncsc.gov.uk/smallbusiness>
6. Verizon Breach Report
 - <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>
7. Vertical Structure
 - <https://www.verticalstructure.com>



VerticalStructure

Questions?

Simon.Whittaker@verticalstructure.com