# Basic Digital Security

## A compilation of resources

**Webinar developed by Deborah Meibergen - June 2020**

# Overview

## Topics

1. Introduction: intro, risk groups & FOSS vs proprietary
2. Threat modeling
3. Operating Systems (including disk encryption and backups)
4. Mail, PGP (encryption) and infrastructure
5. Be secure online
6. Password manager(s)
7. Phishing, malware & ransomware
8. Anti-virus software
9. File sharing and Storage
10. Resources

# Introduction

# 1. Introduction

The importance of digital security

The Internet is everywhere both in public and in private life. It is a vital means for professional and personal - often confidential - communication. The internet and how it’s built is complex and there are a lot of weak spots that can be taken advantage of. Therefore it’s important to take basic preventative measures.

# Introduction

## Risk groups

**Risk groups:** Due to nature of the work of NGO's, journalists and activists security risks are an unfortunate reality, and something to be mindful of.

**Threat models**: A threat model is a process that needs to happen on the operational level of an organisation, but it also something you as a journalist or activist need to think about; what are your personal risks and which vulnerabilities can be a threat for you personally, and your work.

**Surveillance and censorship:** are common issues as well, and there can be many adversaries out there that have an incentive to stop you from doing your work.

This varies from **black hat hackers**, -who have ill-intent,- to governments, and not just from countries with censorship issues. **Freedom of speech** is more and more under pressure. Take what control you have to push back. Every little bit helps.

# Introduction

## Open source vs proprietary software

- Open-source refers to the software whose source code is available for anybody to access and modify, while proprietary software refers to the software which is solely owned by the individual or publisher who developed it.

- Manufacturers of proprietary, closed-source software are sometimes pressured building in backdoors or other covert, undesired features into their software. Instead of having to trust software vendors, users of FOSS can inspect and verify the source code themselves and can put trust on a community of volunteers and users. As proprietary code is typically hidden from public view, only the vendors themselves and hackers may be aware of any vulnerabilities in them while FOSS involves as many people as possible for exposing bugs quickly.

- Licenses of proprietary software are often expensive and a company has so much reliance on the software as well as data running on these platforms that they are stuck in a so called “vendor-lock-in” which is next to impossible to get out of.

# Threat Modeling

# Threat modeling

## Risk assessment and operational security

Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.

Threat modeling happens on organisational level, or is something you need to be mindful of when you are working as a freelancer.

# Threat modeling

## Risk assessment and operational security

The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.

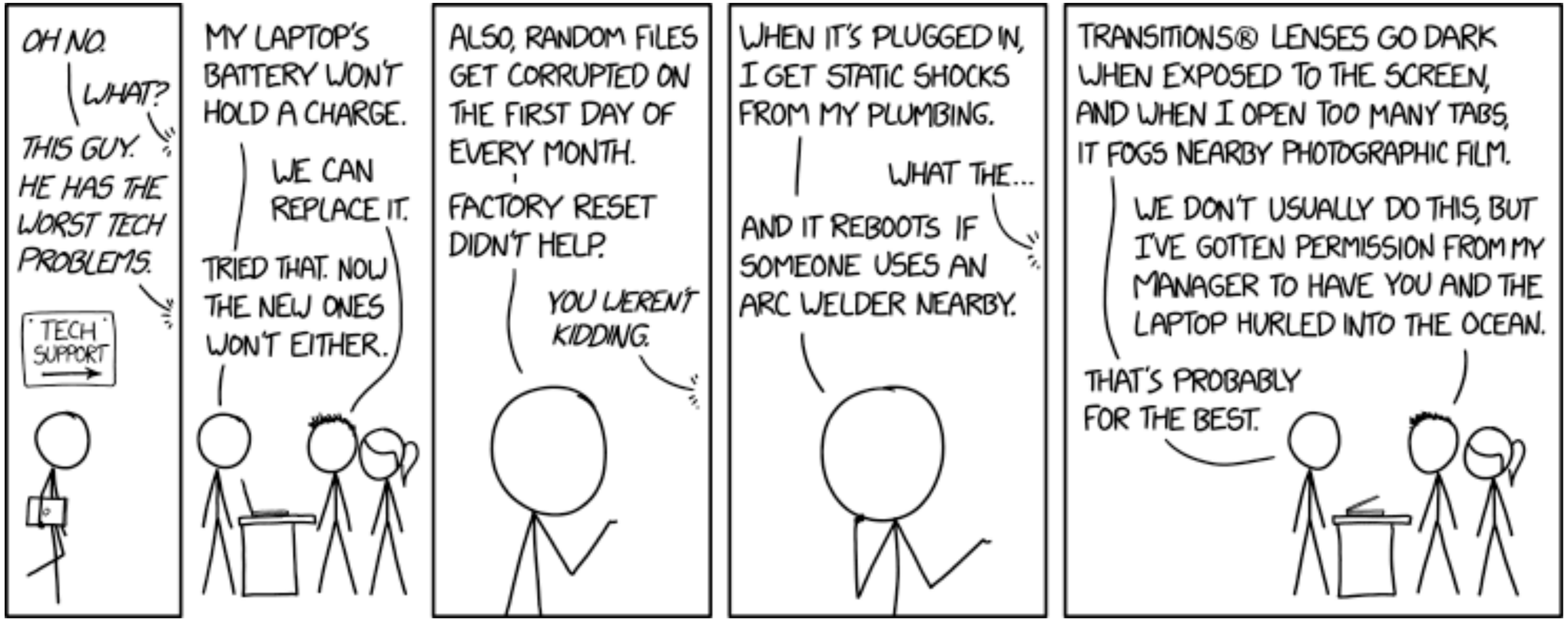
Threat modeling answers questions like *“Where am I most vulnerable to attack?”*, *“What are the most relevant threats?”*, and *“What do I need to do to safeguard against these threats?”*.

# Operational Security

## Important things to assess

- Who is your adversary?
- What do you need to protect?
- Data storage and transit security: How and where is data stored, and how is this protected?
- Communication security: Conducting communication over minimally secure channels is something to look out for. For end-to-end guarantees the organisation can use e-mail encryption with PGP, but also Signal, and using disk encryption and secure file sharing and storage such as Nextcloud or trusted hardware (e.g. by using an independent service provider)
- Data deletion policies: Is there a secure data deletion processes in place when data is deleted and / or destroyed?

# Operating Systems


OH NO.
WHAT?
THIS GUY. HE HAS THE WORST TECH PROBLEMS.
TECH SUPPORT
MY LAPTOP'S BATTERY WON'T HOLD A CHARGE.
WE CAN REPLACE IT.
TRIED THAT. NOW THE NEW ONES WON'T EITHER.
ALSO, RANDOM FILES GET CORRUPTED ON THE FIRST DAY OF EVERY MONTH.
FACTORY RESET DIDN'T HELP.
YOU WEREN'T KIDDING.
WHEN IT'S PLUGGED IN, I GET STATIC SHOCKS FROM MY PLUMBING.
WHAT THE...
AND IT REBOOTS IF SOMEONE USES AN ARC WELDER NEARBY.
TRANSITIONS® LENSES GO DARK WHEN EXPOSED TO THE SCREEN, AND WHEN I OPEN TOO MANY TABS, IT FOGS NEARBY PHOTOGRAPHIC FILM.
WE DON'T USUALLY DO THIS, BUT I'VE GOTTEN PERMISSION FROM MY MANAGER TO HAVE YOU AND THE LAPTOP HURLED INTO THE OCEAN.
THAT'S PROBABLY FOR THE BEST.

# 2. Operating Systems

## Desktops, laptops and mobile phones

- Keep your system and phones OS’es up-to-date
- Windows, OSX, Linux and security risks vs usability
- Disk encryption
- Backups

# OS updates

Keep your operating system up-to-date: the **developers of operating systems provide updates** that you should install from time to time.

These may be automatic or you may have to request them by entering a command or adjusting your system settings. Some of these updates **make your computer more efficient and easier to use**, and others **fix security holes**.

# OS updates

**Attackers** learn about these security holes rapidly, sometimes even before they are fixed, so fixing them promptly is crucial. Luckily, most operating systems do a quite good job in keeping the system updated and safe, if at least you allow them to do so. **Installing new updates** on a new computer is very important.

A new computer you buy in the shop, can be there for some months already. This means the computer is often behind with the security updates. So when **buying a new computer**, please **take some time to update** your Operating System.

# Windows, OSX & Linux

Windows is the most common operating system, but also the most vulnerable. Most viruses have been written for Windows because so many people use it. Make sure to always update your system if you are prompted, and even better is to assure yourself you have automatic updates switched on.

# Update settings

- Windows: https://support.microsoft.com/en-us/help/311047/how-to-keep-your-windows-computer-up-to-date
- OSX: https://support.apple.com/guide/mac-help/get-macos-updates-mchlpx1065/10.14/mac/10.14
- Linux: https://linuxize.com/post/how-to-set-up-automatic-updates-on-ubuntu-18-04/ (or search for other distro)

# Mobile phones

## iOS & Android

Make sure to have the settings icon in a visible spot so you can see when there is a new update. Always do the update as soon as you can. Backup your phone on your computer and proceed with the update by following the instructions.

# Settings iOS & Android

You can check your update settings here:

- iOS: https://support.apple.com/en-us/HT204204
- Android: https://support.google.com/android/answer/7680439?hl=en

# Disk Encryption

**What is disk encryption and why is it important?**

It helps prevent unauthorised access to the information on your startup disk and protects data on the system. All operating systems have a standard disk encryption functionality built in, but there are also other tools you can use that offer more extended possibilities.

# Disk Encryption

**4 reasons**

1. Security (especially important for laptops)
2. It’s easy to apply
3. Peace of mind (especially when device is stolen)
4. Auditing / compliance (most common at corporations)

# Disk Encryption settings

**You can find the settings for disk encryption on your operating system here:**

- Windows: https://support.microsoft.com/en-us/help/4502379/windows-10-device-encryption
- Veracrypt for Windows: https://securityinabox.org/en/guide/veracrypt/windows

- OSX File Vault: https://support.apple.com/en-us/HT204837
- Veracrypt for Mac: https://securityinabox.org/en/guide/veracrypt/mac

- Linux cryptsetup: https://wiki.archlinux.org/index.php/Dm-crypt/Device_encryption

Providers that offer great software are:

- Veracrypt: https://www.veracrypt.fr/en/Home.html
- Tutorial: https://securityinabox.org/en/guide/veracrypt/linux

# Backups

**Are essential!**

Backups can be used to recover data after its loss from data deletion or corruption, or to recover data from an earlier time. But, it’s also an important security measure in case of Ransomware. More on Ransomware later.

https://en.wikipedia.org/wiki/Backup

# Backups

## How to

Turn on automatic backups when possible!

Windows: https://support.microsoft.com/en-us/help/17127/windows-back-up-restore & https://lifehacker.com/how-to-back-up-your-computer-automatically-with-windows-1762867473
OSX: https://support.apple.com/mac-backup
Linux: https://www.tecmint.com/linux-system-backup-tools/

# Mail and secure infrastructure

# Mail

## It’s complicated

Mail is complicated by its sheer nature, but also to run and maintain. Many organisations have managed mail services from ISP’s, Microsoft 365 (Outlook) or Google (evil but it works like a charm!). Running your own mail server needs a dedicated and skilled sysadmin, so many companies and organisations use a service provider, which is also handy for SLA’s which ensure uptime, otherwise your sysadmin needs to be on call, and monitor the network 24/7.

# Mail

## Independent infrastructure & providers

If hardware is owned (and thus bought and managed) by the providers themselves, and where the hardware is located plays a huge role in security, due to local laws and legislation. Mail and infrastructure is a dense and complicated topic, not suitable for this webinar.

# Mail

## Independent providers for NGO’s

A good example of independent service providers and thus more trustworthy parties for organisations (NGO, independent media) are: Greenhost, Virtual Road (Qurium), May First and 1984 (Iceland).

# Mail

## Independent providers for other users

For regular users and small (activists) groups that need secure (hardware, data logging and location-wise), e2e encrypted mail, please look at: Riseup, ProtonMail and Tutanota.

# Mail

## PGP / GPG: Mail encryption

Mail can be made more secure by using PGP. Pretty Good Privacy (**PGP**) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It can take some time to set up and use but it has upsides (confidentiality, digital signatures and web of trust) as well as downsides (hard to use and next to impossible to use on mobile phone).

# Mail

## How to use encryption

It’s not trivial to use PGP at first, but it’s definitely not impossible! Creating keys and how to use the tool works best when doing it together on the spot, but because this is a webinar, you can try it yourself. Use this website to find your mail client and take it from there: https://www.openpgp.org/software/

# Update PGP August 2020

## Protocol and key servers

My cryptographer friend Harry Halpin said:

“I've stopped using PGP and SO SHOULD YOU. It's not just usability, but due to fundamental problems with the protocol itself. Just use Signal or Matrix/OTR”
Thread: https://twitter.com/harryhalpin/status/1299276179858501632

# HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:


IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

# PGP fingerprint

**Use this to verify my public key**

My PGP fingerprint if you want to find me and verify my public key:

B5EA B655 B966 6828 775B 1AD5 B4E5 8B06 B933 70D0

# A small part of my public key

## Just cause it looks cool :)


-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFfkygoBEAC7UwVhEKK+4XFii22ZuZaMncV9tu+jZW9BXhdq3cisGs5vcUuS
kE2+ZyGG8y//9vv0iAsK5Ev5NHKQZhH5my3EcgkMOc9zir/WBgjJUaB0fF5KHS4V
w9kXA3vibkzajVpQ4JoYBmUU+NXwNTeuvvjLXK35dqf3/J2K391xr7fPzhk5GfET
FmceiWhrVGkKWOmvIuV5x/z+2l2yhn6GuKdWLhB4jx9jyiGSccAVP3piPAV0H8ob
r1TmtzshwvkosyunRCY4Jj4JTUAhYS8JjUGMt44+ce/ZgqpM1yuUt58SRYn1Z0cr
I3rF0YSNRdT2DIAEbv2lDdsMQY/2sio++HEv3TpiR/40bF8qpYk50jQ/cly5Qneo
o7w6ZXkKSqM2p7+EJVNquz0OEOPZ9QEnlhhH4/3SGskoaBzvEaJPD/fUHywgf8hk
3k73lS4OJaMsDvn3cZdZcyqJER9Af5YE9X1H4WlCLd4HEsr5BvkacZEjCYX+rfJF
Stxy8k3KFMGAf3RqUNyqHl2Ge4AKrBG5ufvNnXnB4zpFdsQ6V+Of6olJAOpZl3Fz
9DbaZaj4WcG/w5Ih4Qw0O1zy7GCkdkTqt33ffIL9kusUhaPmaidumPwLYoDe7SKm
vcy7fdfxiUdlwfDWl4Q/BGE5X1jEueGSCfnSLObrt9qCytUJFnWqzHB8jwARAQAB
tCJEZWJvcmFoIE1laWJlcmdlbiA8ZGVtQHJpc2V1cC5uZXQ+iQI9BBMBCgAnBQJX
5MoKAhsjBQkJZgGABQsJCAcDBRUKCQgLBRYCAwEAAh4BAheAAAoJELTliwa5M3DQ
H8AQALNXRZqQjpGPM5JWKXvEe3S82gPwq2TPilFh9y+XoulpwpwgsKAfjh+81Dxi
02ICiWxr6r2IWwKTD8Ilyq17ORGxSzdta367PS8fGGnV19mQFhQ+8d1TJxBJLBSW
2LA26sv6tyB+UR1TVo/5cq+fBmnQcTUnTY31TTJ9cehmdsO+42kX7bFI0mmOrsOh
6HMruKx3aoGhgHdVTN5BateXaptydJeCKQAw/weq3oxs6C3uhsimh5pjFi48f9/b

# Be Secure Online

# 3. Be Secure Online

## Smart but simple tactics

- VPN’s: which provider to pick and what to look for why
- Using WiFi in cafe’s, airports or other unknown or untrusted places
- Preferred browser (Firefox, Chrome, and Brave)
- Search engine (DuckDuckGo!)
- Delete history and cookies
- Set browser passwords when saving passwords there, too
- Browser plug-ins and add-ons
- Tor: why, when and where
- 2FA

# VPN’s

A **virtual private network** (**VPN**) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

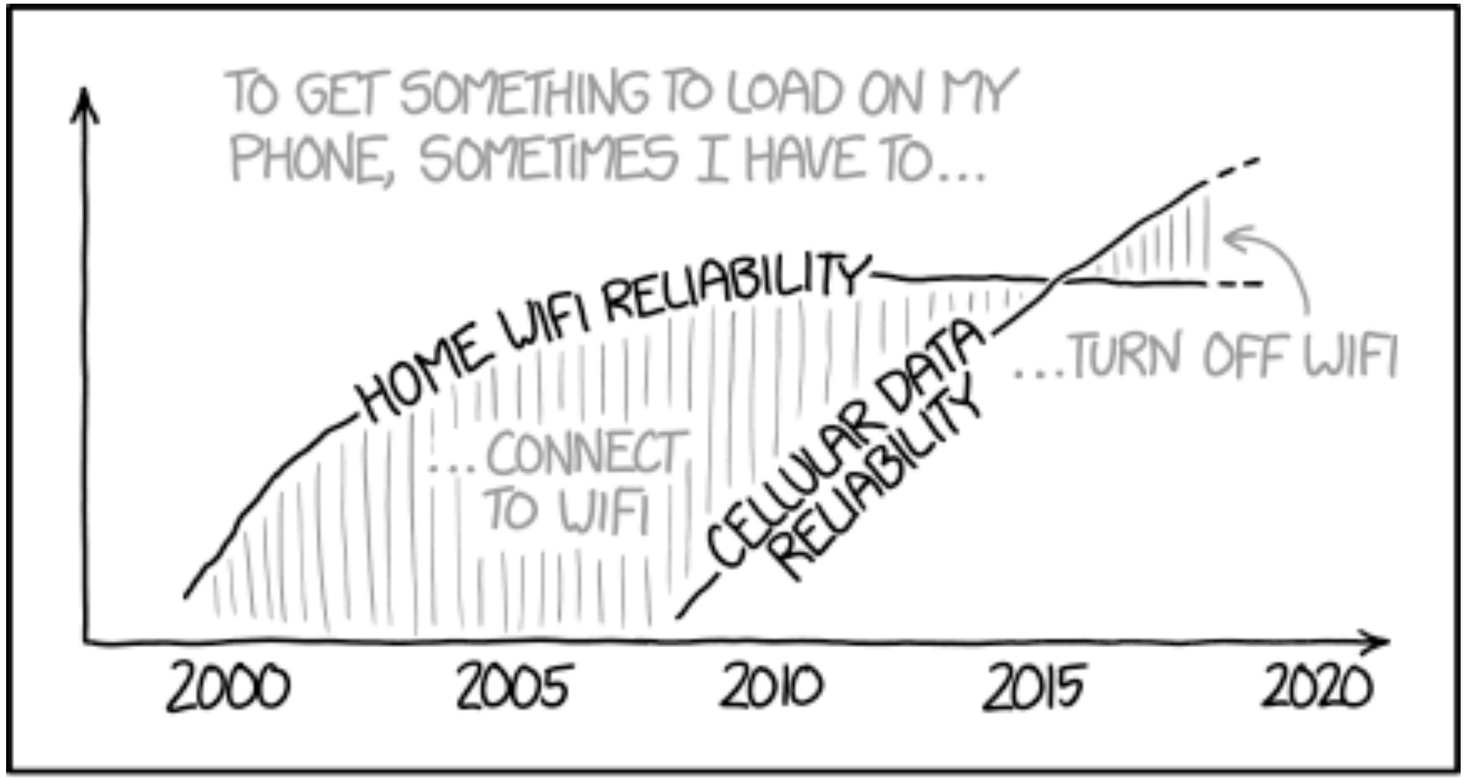
Use a good VPN provider. A free VPN is not a good sign, because free never really means free, there’s always a trade-off. Please, try to steer clear of that.

# Public WiFi

In general, using public Wi-Fi is a lot safer than it was in the early days of the Internet. With the widespread adoption of HTTPS, most major websites will be protected by the same encryption regardless of how you connect to them. For additional security use your VPN.

What about the risk of governments scooping up signals from “open” public Wi-Fi that has  no password? Governments that surveil people on the Internet often do it by listening in on upstream data, at the core routers of broadband providers and mobile phone companies. If that’s the case, it means the same information is commonly visible to the government whether they sniff it from the air or from the wires.

https://www.eff.org/deeplinks/2020/01/why-public-wi-fi-lot-safer-you-think




IT SEEMS WEIRD FROM A NETWORKING POINT OF VIEW, BUT SOMETIME IN THE LAST FEW YEARS THIS FLIPPED FOR ME.

# VPN’s: Picking a provider

Look for the following things when deciding which provider you pick:
- Amount and location of servers
- Privacy and logging policies is an essential step. No logging is the best.
- Additional protocols such as Wireguard
- How many devices can you connect

I recommend Mullvad. Independent provider from the digital human rights community. Affordable (5 EUR) per month and with one account you can use it on 3 different computers, phones.

https://mullvad.net/en/

# Browser Choices

These days most of our use of the internet happens through a web browser, and which one you use has real impacts on your safety online. Besides advertisers trying to track your online activity, there are also adversaries who may try to exploit bugs in your browser in order to compromise your entire system (regardless of which browser you do choose, it’s always important to ensure you have the latest update).

# Browser Choices

There are quite a few different options across various operating systems and devices, so it can be difficult to determine which one is right for you. We're looking for browsers that provide good network security, protect your privacy, and maintain the user experience you expect.

- Firefox: https://www.mozilla.org/en-US/firefox/new/
- Brave: https://brave.com/download/
- Chrome: https://www.google.com/chrome/
- Safari and Internet explorer: Rather not :)

# Search engine

We all know and use Google. She’s a beautiful beast and works very well. But, there’s an alternative; DuckDuckGo.

DuckDuckGo works in broadly the same way as any other search engine, Google included. It combines data from hundreds of sources including Wolfram Alpha, Wikipedia and Bing, with its own web crawler, to surface the most relevant results. Google does exactly the same, albeit on a somewhat larger scale. The key difference: DuckDuckGo does not store IP addresses or user information.

# What are cookies?

An **HTTP cookie** (also called **web cookie**, **Internet cookie**, **browser cookie**, or simply **cookie**) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past). They can also be used to remember pieces of information that the user previously entered into form fields, such as names, addresses, passwords, and credit-card numbers.

Source: https://en.wikipedia.org/wiki/HTTP_cookie

TO PROVE YOU'RE A HUMAN, CLICK ON ALL THE PHOTOS THAT SHOW PLACES YOU WOULD RUN FOR SHELTER DURING A ROBOT UPRISING.

# Deleting history & cookies

Your browser tends to hold onto information, and over time it could cause problems with logging in or bringing up websites. It's always a good idea to clear out the cache, or browser history, and clear cookies on a regular basis. The drawback to this is that your saved usernames and passwords will be deleted and you'll need to re-enter them. But on the plus side, your privacy is more secure and your browser will work better. How to:

- Firefox: https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox
- Brave: https://www.howto-connect.com/clear-history-brave-browser-delete-cache-cookies/
- Chrome: https://support.google.com/accounts/answer/32050?
- https://support.google.com/chrome/answer/95647?

# Browser Master Password

It’s best to only use a password manager. But, if you want to save the passwords in your browser you can, but please set a good master password. Use your password manager to generate a password, or create one with Diceware.

Instructions to set browser password for:

- Firefox: https://support.mozilla.org/en-US/kb/use-master-password-protect-stored-logins
- Brave: https://support.brave.com/hc/en-us/articles/360018185951-How-do-I-use-the-built-in-password-manager-
- Chrome: https://support.google.com/chrome/answer/95606?

# Plug-ins & add-ons

A browser extension is something like a plugin for your browser that adds certain functions and features to it. Extensions can modify the user interface or add some Web service functionality to your browser.

# uBlock Origin

uBlock Origin: is a free and open-source, cross-platform browser extension for content-filtering, including ad-blocking.

- For Chrome: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?
- For Firefox: https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/

# NoScript

NoScript is, essentially, a Firefox add-on that disables things like JavaScript from running on web sites you visit. So before we talk about NoScript, we should actually talk about JavaScript: the programming language that makes the web we have today possible. There have been a few browser vulnerabilities that were exploited via JavaScript. Disabling JavaScript also prevents some types of ads from loading. We don't encourage blocking ads, but if you must, there are better ways to do so than disabling JavaScript altogether.

- For Chrome: https://chrome.google.com/webstore/detail/noscript/doojmbjmlfjjnbmnoijecmcbfeoakpjm?
- For Firefox: https://addons.mozilla.org/en-US/firefox/addon/noscript/

# EFF Tools

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.

Encrypt the web: Install HTTPS Everywhere:
https://www.eff.org/https-everywhere
Privacy Badger automatically learns to block invisible trackers:
https://privacybadger.org/

# Tor

Tor Browser is the best option when it comes to safeguarding your privacy. This hardened version of Firefox is designed to protect user privacy by reducing the amount of unique bits specific to your browsing experience. By limiting the amount of browsing data you share with third parties, Tor Browser effectively prevents trackers from uniquely identifying or fingerprinting you.

https://www.torproject.org/

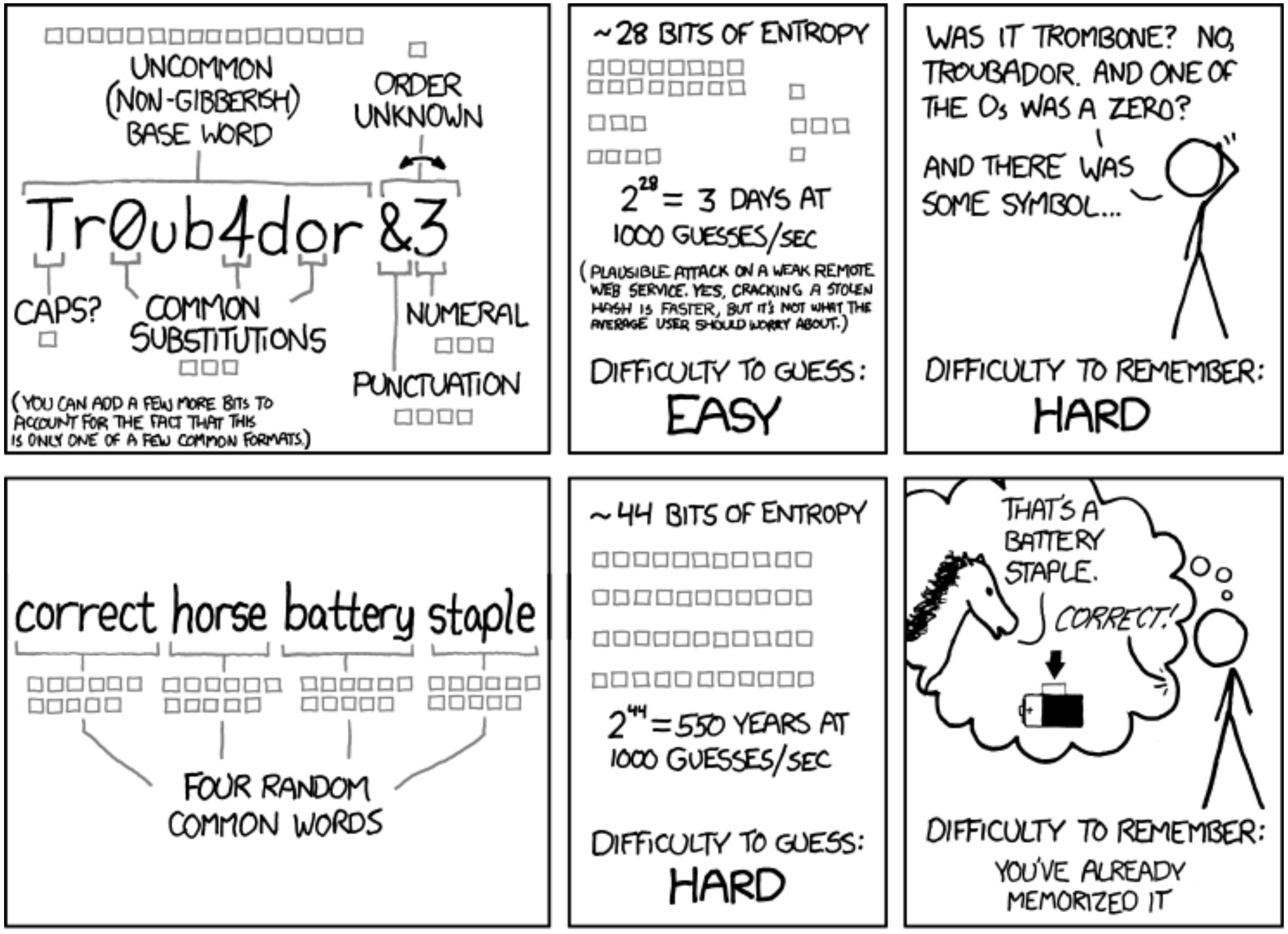
# 2FA

Multi-factor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. It confirms users' claimed identities by using a combination of *two* different factors: 1) something they know, 2) something they have, or 3) something they are.

# 2FA

- SMS codes
- Email codes
- Authentication apps: https://gizmodo.com/the-best-authenticator-apps-for-protecting-your-account-1840711013

# Password Managers




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.

# 4. Password Managers

## Best Practices

- Why it’s important
- Choice of manager: free vs paid, differences, focus on KeepassXC
- Master passphrase, and why this is the most important passphare you’ll ever pick
- Fun way to create a incredibly solid, but easy to remember master passphrase: Diceware

# Why is it important?

The risks of picking passwords by yourself, how easy these passwords can be ‘cracked’ and why you as a human can never be random, even if you think you are.

Secret services like e.g. the NSA have capabilities to easily crack your passwords.

But also (black hat) hackers or others with ill-intent can dump your passwords on the internet for everyone to grab thus comprising your online security.

# Example of a good password

Longer non-dictionary passwords/phrases take exponential longer to crack. Below you see an example of a password that is very difficult to crack, nor remembered :)

%ED+?33~*8fVXHZ5=z_G46CoZw/L{{,adSFF\6ft

And this is how a Diceware passphrase looks (more on Diceware a few slides ahead):

bazooka chubby emission junkyard muskiness pentagram record thrift

# Which password manager?

Free (open source) services and paid services. Not all are created equally but each service is as safe as the master passphrase you set. That said, data breaches have happened in the past. For example, the popular service LastPass.

https://www.forbes.com/sites/daveywinder/2019/09/16/google-warns-lastpass-users-were-exposed-to-last-password-credential-leak/#745e004a4600

# Which password manager?

We will focus on KeePassX which is an open-source tool for Windows, iOS and Linux. You can download and install it from here:

- Windows: https://keepassxc.org/download/#windows
- iOS: https://keepassxc.org/download/#mac
- Linux: https://keepassxc.org/download/#linux

# Password manager on mobile

There’s no formal release of KeePassX for iOS but there are options: https://keepassium.com/articles/keepass-apps-for-ios/

For Android: https://keepass.info/download.html

Please do some research into these apps before installing them. I’m not in the know enough to make a recommendation.

I don’t carry my passwords on my phone. Yes, this meant I opened all apps and manually typed in the passwords from my desktop / laptop database :)

Commercials products like 1password and LastPass do have well-working mobile apps.

# Diceware

Fun way to create a solid, easy to remember master passphrase!

What is Diceware, briefly explained: Diceware is a method for creating passphrase, passwords and other cryptographic variables using ordinary dice as a hardware random number generator. For each word in the passphrase, five rolls of the dice are required. The numbers from 1 to 6 that come up in the rolls are assembled as a five-digit number, e.g. *43146*. That number is then used to look up a word in a word list. In the English list *43146* corresponds to *munch*. By generating several words in sequence, a lengthy passphrase can be constructed.

# Diceware links

- The Intercept article on Diceware (fun to read!): https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/

- Diceword word list: https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt

# Phishing, malware & ransomware

# 5. Phising, malware & Ransomware

**What is it, what to watch out for: “when in doubt, don’t do it”**

- Social Engineering
- What is phishing?
- What to look for
- Phishing guides
- What is malware
- Ransomware

# Social Engineering

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

https://en.wikipedia.org/wiki/Social_engineering_(security)

# What is Phishing?

On your path to improving your digital security, you may encounter bad actors who attempt to undermine your security goals. We call these bad actors adversaries. When an adversary sends an email or link that looks innocent, but is actually malicious it’s called phishing.

A phishing attack usually comes in the form of a message meant to convince you to:

- click on a link;
- open a document;
- install software on your device; or
- enter your username and password into a website that’s made to look legitimate.

# Phishing: what to look for

Phishing emails and text messages may look like they’re from a company you know or trust. They may look like they’re from a bank, a credit card company, a social networking site, an online payment website or app, or an online store. Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment.

# Phishing: what to look for

They may:

- say they’ve noticed some suspicious activity or log-in attempts
- claim there’s a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you’re eligible to register for a government refund
- offer a coupon for free stuff

# Phishing: what to look for

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: Do I have an account with the company or know the person that contacted me?

# Phishing: what to look for - 1

## 5 clues

**1. The message is sent from a public email domain**

No legitimate organisation will send emails from an address that ends ‘@gmail.com’. Not even Google. Most organisations, except some small operations, will have their own email domain and company accounts. For example, legitimate emails from Google will read ‘@google.com’. If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate. The best way to check an organisation’s domain name is to type the company’s name into a search engine. This makes detecting phishing seem easy, but cyber criminals have plenty of tricks up their sleeves to deceive you.

*Top tip: Look at the email address, not just the sender*

# Phishing: what to look for - 1

## 5 clues

Many of us don’t ever look at the email address that a message has come from. Your inbox displays a name, like ‘IT Governance’, and the subject line. When you open the email, you already know (or think you know) who the message is from and jump straight into the content.

When crooks create their bogus email addresses, they often have the choice to select the display name, which doesn’t have to relate to the email address at all.

They can, therefore, use a bogus email address that will turn up in your inbox with the display name Google. But criminals rarely depend on their victim’s ignorance alone. Their bogus email addresses will use the spoofed organisation’s name in the local part of the address.

# Phishing: what to look for - 2

## 5 clues

**2. The domain name is misspelt**

There’s another clue hidden in domain names that provide a strong indication of phishing scams – and it unfortunately complicates the previous clue. The problem is that anyone can buy a domain name from a registrar. And although every domain name must be unique, there are plenty of ways to create addresses that are indistinguishable from the one that’s being spoofed.

*You don’t need to fall victim to help criminal hackers*

# Phishing: what to look for - 3

## 5 clues

**3. The email is poorly written**

You can often tell if an email is a scam if it contains poor spelling and grammar. Many people will tell you that such errors are part of a ‘filtering system’ in which cyber criminals target only the most gullible people.

The theory is that, if someone ignores clues about the way the message is written, they’re less likely to pick up clues during the scammer’s endgame. However, this only applies to outlandish schemes like the oft-mocked Nigerian prince scam, which you have to be incredibly naive to fall victim to.

That, and scams like it, are manually operated: once someone takes to the bait, the scammer has to reply. As such, it benefits the crooks to make sure the pool of respondents contains only those who might believe the rest of the con. But this doesn’t apply to phishing.

# Phishing: what to look for - 3

## 5 clues

**Automated attacks**

With phishing, scammers don’t need to monitor inboxes and send tailored responses. They simply dump thousands of crafted messages on unsuspecting people. As such, there’s no need to filter out potential respondents. So why are so many phishing emails poorly written? The most obvious answer is that the scammers aren’t very good at writing.

Remember, many of them are from non-English-speaking countries and from backgrounds where they will have limited access or opportunity to learn the language. With this in mind, it becomes a lot easier to spot the difference between a typo made by a legitimate sender and a scam.

*Top tip: Look for grammatical mistakes, not spelling mistakes*

When crafting phishing messages, scammers will often use a spellchecker or translation machine, which will give them all the right words but not necessarily in the proper context.

# Phishing: what to look for - 4

## 5 clues

### 4. It includes suspicious attachments or links

Phishing emails come in many forms. We've focused on emails in this article, but you might also get scam text messages, phone calls or social media posts.

But no matter how phishing emails are delivered, they all contain a payload. This will either be an infected attachment that you're asked to download or a link to a bogus website. The purpose of these payloads is to capture sensitive information, such as login credentials, credit card details, phone numbers and account numbers.

# Phishing: what to look for - 4

## 5 clues

### What is an infected attachment?

An infected attachment is a seemingly benign document that contains malware. In a typical example, like the one below, the phisher claims to be sending an invoice.

Also look out for suspicious links. Check the destination address by hoovering over the link, if not written out. Don’t click on it though.

# Phishing: what to look for - 5

## 5 clues

**5. The message creates a sense of urgency**

Scammers know that most of us procrastinate. We receive an email giving us important news, and we decide we'll deal with it later. But the longer you think about something, the more likely you are to notice things that don't seem right.

Maybe you realise that the organisation doesn't contact you by that email address, or you speak to a colleague and learn that they didn't send you a document. Even if you don't get that 'a-ha' moment, coming back to the message with a fresh set of eyes might help reveal its true nature. That's why so many scams request that you act now or else it will be too late. This has been evident in every example we've used so far.

# Phishing Guides

Phishing attacks can trick you into giving up your passwords or trick you into installing malware on your device. Attackers can use malware to remotely control your device, steal information, or spy on you.

Guides and tips:

- https://ssd.eff.org/en/module/how-avoid-phishing-attacks
- https://www.eff.org/deeplinks/2020/03/phishing-time-covid-19-how-recognize-malicious-coronavirus-phishing-scams

# What is Malware?

Malware is software written in order to steal information or to use your computer for other purposes. Malware is the collective name for a number of malicious software variants, including viruses, ransomware, spyware and computer worms (a stand-alone malware computer program). Shorthand for malicious software, malware typically consists of code developed by cyber-attackers, designed to cause extensive damage to data and systems or to gain unauthorised access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

The most fascinating malware (thus far) Stuxnet - an article and documentary:

- https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
- https://www.npostart.nl/2doc/04-10-2019/VPWON_1309553

# What is Ransomware?

Ransom malware, or ransomware is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

Article I wrote at Greenhost on this topic in 2016 - still accurate:
https://greenhost.net/blog/2016/03/16/ransomware-on-our-doorstep/

# Anti-virus Software

# 6. Anti-virus Software

## What are viruses?

A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

- https://en.wikipedia.org/wiki/Computer_virus

Why they are mostly targeting Windows systems

- Windows Defender is important
- For other operating systems, just be mindful of your digital ‘hygiene’

# How do viruses work?

If you're using Microsoft Windows, use anti-virus software (Windows Defender) and keep it updated. Viruses and malware can gain access to your system, make changes and hide themselves. They could be sent to you in an e-mail, be on a Web page you visit, or be part of a file that does not appear to be suspicious. Anti-virus software providers constantly research emerging threats and add them to lists of things that your computer will block. In order to allow the software to recognise new threats, you must install updates as they are released.

For other operating systems just make sure you follow the advice from this webinar and risks will be much lower.

# File sharing & storage

# 7. File sharing and Storage

## Available tools and tips

Why file sharing and storage is so important. Pros and cons of common tools: open-source tools vs proprietary tools.

- iCloud
- Google Drive
- Dropbox
- Use Nextcloud or Onionshare!

# Resources

## FLOSS, tips and general information

https://archive.flossmanuals.net/_booki/basic-internet-security/basic-internet-security.pdf

https://ssd.eff.org/en#index

https://safetag.org/guide/

https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email

https://en.wikipedia.org/wiki/Free_and_open-source_software

https://freedom.press/training/-depth-guide-choosing-web-browser/

http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/

https://www.howtogeek.com/138865/htg-explains-should-you-disable-javascript/

All images all from: https://xkcd.com/license.html <3