Digital Self-Defence

Levelling up your defence in a world
that is levelling up its offence.

Jonas Betzendahl, M.Sc.

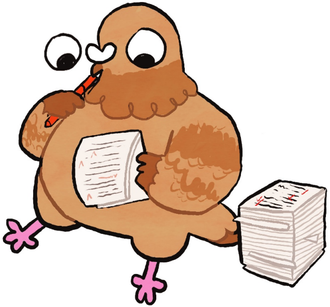
2019 – 12 – 06

@lambdaTotoro (@chaos.social)

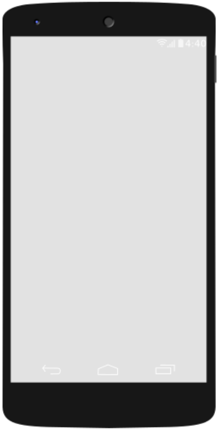
Who am I?

Jonas Betzendahl
`lambdatotoro@posteo.de`

- Bielefeld University
  Cognitive Informatics + Intelligent Systems
- Now @ FAU Erlangen-Nürnberg
  Knowledge Representation and Management
- Love for teaching and science communication
- Favourite topics: misconceptions about and risks of technology.

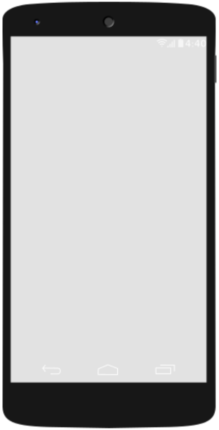


Who are you?



I have no idea who you are! But I'm making a few assumptions. In all likelihood, you ...

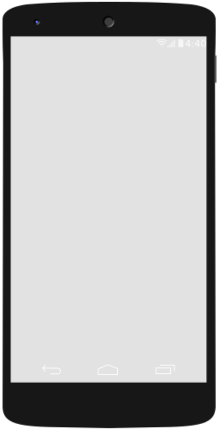
Who are you?



I have no idea who you are! But I'm making a few assumptions. In all likelihood, you . . .

- *don't* necessarily have a degree in computer science or a related field.

Who are you?



I have no idea who you are! But I'm making a few assumptions. In all likelihood, you . . .

- *don't* necessarily have a degree in computer science or a related field.
- *do* regularly interact with computers, probably both professionally and privately.

What is the problem?

Before we can talk about digital *self-defence*, we need an idea about digital *violence*.

What is the problem?

Before we can talk about digital *self-defence*, we need an idea about digital *violence*.

`Digital violence is all violence that uses digital tools (computers, phones, apps,...), digital media (video, email,...) or occurs within online spaces.`

What is the problem?

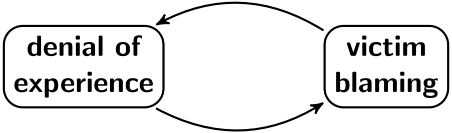
Before we can talk about digital *self-defence*, we need an idea about digital *violence*.

Digital violence is all violence that uses digital tools (computers, phones, apps,...), digital media (video, email,...) or occurs within online spaces.

We believe that usually, digital violence does not happen in isolation from "analogue violence" but often forms an addition to or a continuation of preexisting violent contexts.

What is *not* the solution?

A common problem that is making things worse:

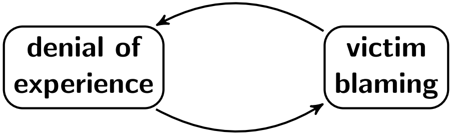


denial of experience

victim blaming

What is *not* the solution?

A common problem that is making things worse:



- “That’s not that bad!”, “It’s not harassment if you can just log off!”, . . .
- “Don’t feed the troll!”, “Don’t take nudes!”, “Don’t be online!”, . . .

What *is* the solution?

Sometimes, sunlight is the best disinfectant.

Many attacks in the digital realm can only work if the victim doesn't know about them, isn't sensitised to them or reacts wrongly to them.

What *is* the solution?

Sometimes, sunlight is the best disinfectant.

Many attacks in the digital realm can only work if the victim doesn't know about them, isn't sensitised to them or reacts wrongly to them.

This workshop is to give you an overview of some of the most important attacks and what to do about them.

What is this workshop?

I will be giving input, but this is *not* a lecture.

I'd rather have a conversation than finish all my slides.

Please ask questions immediately, do feel free to interrupt at any point.

Technical Attacks

Secure Passwords

Passwords are usually the first and most important barrier between our accounts and those that would take them.

Good passwords should resist both *dictionary* and *brute-force* and hence be. . .

- . . . uncommon, ideally unique.
- . . . not too short ($\geq$ 12 characters).
- . . . high-entropy
  (contain letters, numbers, specials).

Passwords (Quiz)

Which of these is the “worst” (cum kilo salis) way to do passwords?

- Using many different weak passwords.
- Using the same strong password on all sites.
- Using many different strong passwords,
  but write them down next to your computer.

Passwords (Quiz)

Which of these is the “worst” (cum kilo salis) way to do passwords?

- Using many different weak passwords.
- Using the same strong password on all sites.
- Using many different strong passwords,
  but write them down next to your computer.

Common Passwords

Any of these ring a bell? The most common passwords. . .

. . . in Germany:

- 123456
- 12345
- 123456789
- ficken
- 12345678

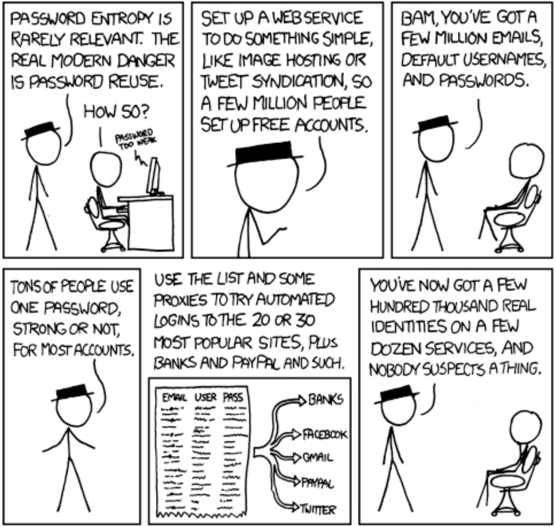
- hallo123
- hallo
- 123
- passwort
- master

. . . worldwide

- 123456
- 123456789
- qwerty
- password
- 111111

- 12345678
- abc123
- 1234567
- password1
- 12345

Password Reuse


PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.
TONS OF PEOPLE USE ONE PASSWORD, STRONG OR NOT, FOR MOST ACCOUNTS.
USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.
EMAIL USER PASS
BANKS
FACEBOOK
GMAIL
PAYPAL
TWITTER
YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.

Passwords from Stories

One way of generating passwords that are easy for humans to remember but hard for computers to guess: Generate a sentence you associate with the website an use all beginning letters plus numbers and punctuation.

Passwords from Stories

One way of generating passwords that are easy for humans to remember but hard for computers to guess: Generate a sentence you associate with the website an use all beginning letters plus numbers and punctuation.

Example Amazon Password:

“**I** **w**ish **J**eff **B**ezos **w**ould **d**o **s**omething **u**seful **w**ith **h**is **110** **B**illion **Dollars!**”

becomes

IwJBwdsuwh110B$!

(crackable in 39555681645472620 years)

Password Managers

Another way of avoiding password reuse while still using strong passwords are *password managers*. These are software secured with one master password that remember all your other passwords. They also can generate secure passwords:

Password Managers

Another way of avoiding password reuse while still using strong passwords are *password managers*. These are software secured with one master password that remember all your other passwords. They also can generate secure passwords:

Like this one:

```
1kgaV|FKkYC?q=p$1WxG9vSL;932Z.h&
```

Password Managers

Another way of avoiding password reuse while still using strong passwords are *password managers*. These are software secured with one master password that remember all your other passwords. They also can generate secure passwords:

Like this one:

```
1kgaV|FKkYC?q=p$1WxG9vSL;932Z.h&
```

There are many options (commercial and open source) for Windows, Mac, Linux, Android, iOS, . . . that can also sync (manually or via cloud) across devices. Also consider analogue ones.

Security Questions (1)

Some sites offer for you to choose a security question for account recovery or even supply one yourself. If this happens, be sure to go for one that is. . .

Security Questions (1)

Some sites offer for you to choose a security question for account recovery or even supply one yourself. If this happens, be sure to go for one that is. . .

- . . . **Safe:** cannot be guessed or researched

Security Questions (1)

Some sites offer for you to choose a security question for account recovery or even supply one yourself. If this happens, be sure to go for one that is. . .

- . . . **Safe:** cannot be guessed or researched
- . . . **Stable:** does not change over time

Security Questions (1)

Some sites offer for you to choose a security question for account recovery or even supply one yourself. If this happens, be sure to go for one that is...

- ... **Safe:** cannot be guessed or researched
- ... **Stable:** does not change over time
- ... **Memorable:** can remember

Security Questions (1)

Some sites offer for you to choose a security question for account recovery or even supply one yourself. If this happens, be sure to go for one that is. . .

- . . . **Safe:** cannot be guessed or researched
- . . . **Stable:** does not change over time
- . . . **Memorable:** can remember
- . . . **Simple:** is precise, simple, consistent

Security Questions (1)

Some sites offer for you to choose a security question for account recovery or even supply one yourself. If this happens, be sure to go for one that is. . .

- . . . **Safe:** cannot be guessed or researched
- . . . **Stable:** does not change over time
- . . . **Memorable:** can remember
- . . . **Simple:** is precise, simple, consistent
- . . . **One of Many:** has many possible answers

Security Questions (1)

Examples of *good* security questions:

- What's the first name of the first person you kissed?
- What's the last name of the teacher that gave you your first failing grade?

Examples of *bad* security questions:

- In what year was your mother born?
- What's your favourite food?

Smartphone Security (Quiz)

Which of these is the safest way of locking your phone?

- A six-digit PIN
- A six-point swipe pattern
- Your fingerprint / face as a biometric pattern

Smartphone Security (Quiz)

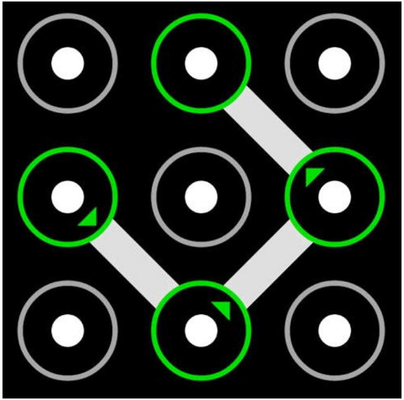
Which of these is the safest way of locking your phone?

- A six-digit PIN
- A six-point swipe pattern
- Your fingerprint / face as a biometric pattern

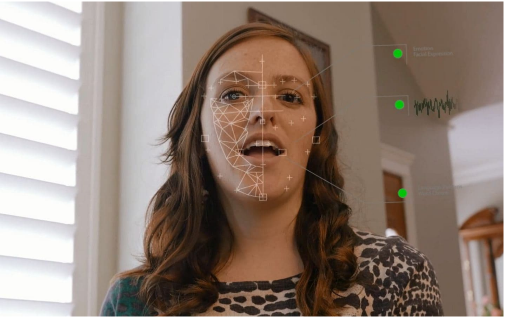
Swipe Patterns

Swipe patterns are not as safe as a pin number of the same length.

Studies have shown they are easier to gleam "over the shoulder" and can sometimes also be reconstructed from smudge marks.



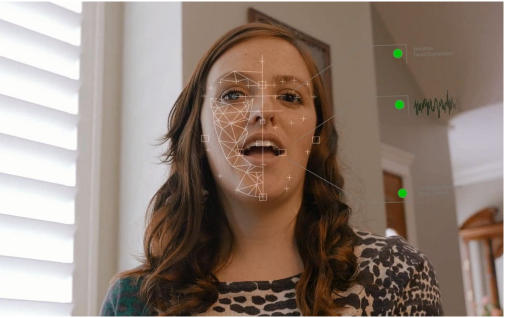
Biometrics



Biometrics (such as fingerprints, facial recognition, . . .) are very convenient!

But they are not good passwords! For example, they can't be . . .

Biometrics

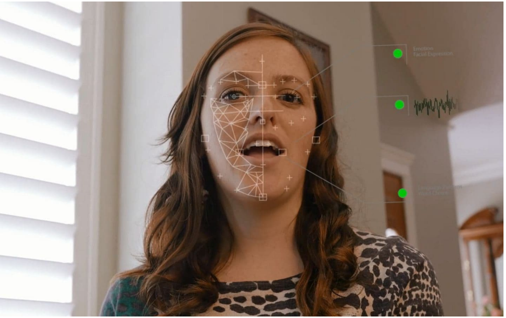


Biometrics (such as fingerprints, facial recognition, . . .) are very convenient!

But they are not good passwords! For example, they can't be . . .

- changed or reset,

Biometrics

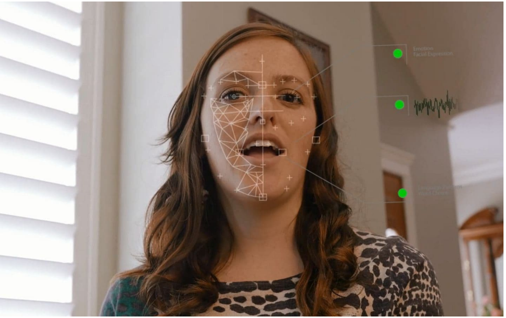


Biometrics (such as fingerprints, facial recognition, . . .) are very convenient!

But they are not good passwords! For example, they can't be . . .

- changed or reset,
- "forgotten",

Biometrics

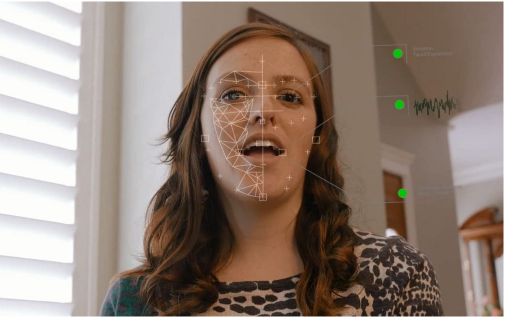


Biometrics (such as fingerprints, facial recognition, . . .) are very convenient!

But they are not good passwords! For example, they can't be . . .

- changed or reset,
- "forgotten",
- fake-proofed

Biometrics



Biometrics (such as fingerprints, facial recognition, . . .) are very convenient!

But they are not good passwords! For example, they can't be . . .

- changed or reset,
- "forgotten",
- fake-proofed

Biometrics are better thought of as *user names*, not *passwords*!

Leaks & Data Breaches

To participate in online culture, you will have to give your information to organisations or companies. Sometimes, through no fault of your own (e.g. the company gets hacked), this data will be compromised and become available to the public.

Leaks & Data Breaches

To participate in online culture, you will have to give your information to organisations or companies. Sometimes, through no fault of your own (e.g. the company gets hacked), this data will be compromised and become available to the public.

There is no real way to “defend” against this, but several good responses (such as changing all changeable information, depending). But first, you need to *know* about it.

Have I been pwned?

Take a few minutes and visit one of these leak detection services:

- `https://haveibeenpwned.com/`
- `https://sec.hpi.de/ilc/`

Enter your own email to see if any of your accounts have been compromised in big leaks in the past. If they have, consider changing your password(s) soon.

If you feel uncomfortable using your own email address, you can use one of mine:

`jonas.betzendahl@gmail.com`

Stalker- & Spouseware

A growing phenomenon in recent years, Stalkerware is monitoring software (often marketed as “catching cheating spouses” or “pet/kid surveillance”) that is installed on the victims phone by an attacker the victim knows.

These kinds of malware can. . .

- . . . forward and record all texts, messages, calls.
- . . . make location data available.
- . . . record video and audio at all times.

Stalker- & Spouseware

A growing phenomenon in recent years, Stalkerware is monitoring software (often marketed as "catching cheating spouses" or "pet/kid surveillance") that is installed on the victims phone by an attacker the victim knows.

These kinds of malware can...

- ...forward and record all texts, messages, calls.
- ...make location data available.
- ...record video and audio at all times.

Kaspersky study:
2019 saw $\geq$ 35% increase worldwide, and a $\geq$ 79% increase in Germany.

How to spot Stalkerware

There is *no* guaranteed way of confirming that you do not have Stalkerware on your phone. However, there are a few common warning signs:

How to spot Stalkerware

There is *no* guaranteed way of confirming that you do not have Stalkerware on your phone. However, there are a few common warning signs:

- High battery usage

How to spot Stalkerware

There is *no* guaranteed way of confirming that you do not have Stalkerware on your phone. However, there are a few common warning signs:

- High battery usage
- Apps, even innocuous-seeming ones, that you don't remember installing.

How to spot Stalkerware

There is *no* guaranteed way of confirming that you do not have Stalkerware on your phone. However, there are a few common warning signs:

- High battery usage
- Apps, even innocuous-seeming ones, that you don't remember installing.
- Apps from unrecognised sources
  Android: Settings ⇒ Security ⇒ Allow unknown sources
  Apple: Jailbroken Phone

How to spot Stalkerware

There is *no* guaranteed way of confirming that you do not have Stalkerware on your phone. However, there are a few common warning signs:

- High battery usage
- Apps, even innocuous-seeming ones, that you don't remember installing.
- Apps from unrecognised sources
  Android: Settings ⇒ Security ⇒ Allow unknown sources
  Apple: Jailbroken Phone
- People in your life that seem to know things they should have no way of knowing.

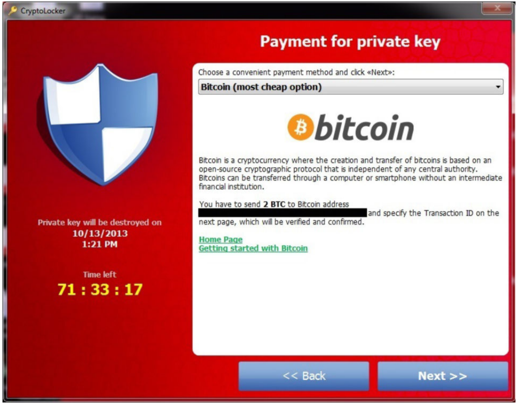
How to spot Stalkerware

There is *no* guaranteed way of confirming that you do not have Stalkerware on your phone. However, there are a few common warning signs:

- High battery usage
- Apps, even innocuous-seeming ones, that you don't remember installing.
- Apps from unrecognised sources
  Android: Settings ⇒ Security ⇒ Allow unknown sources
  Apple: Jailbroken Phone
- People in your life that seem to know things they should have no way of knowing.

It's very difficult to get rid of this malware because it is designed to be resilient and avoid detection. The ultima ratio is a factory reset.

CryptoLockers



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

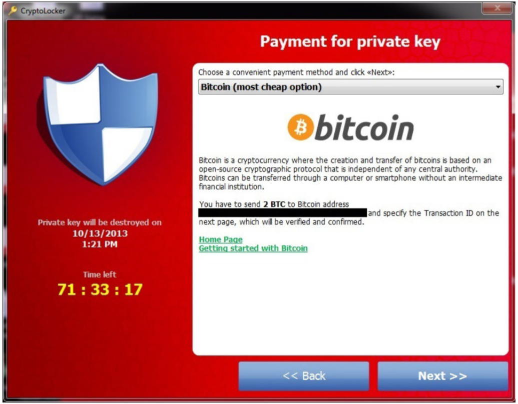
Home Page
Getting started with Bitcoin

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

CryptoLockers / Ransomware encrypts all files on your computer it can find and asks for money.

CryptoLockers



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

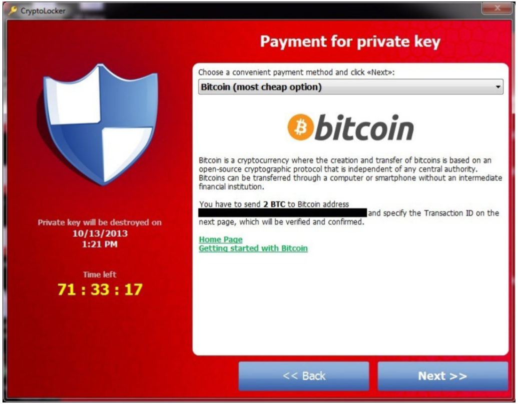
Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

CryptoLockers / Ransomware encrypts all files on your computer it can find and asks for money.

Don't Panic! Research the malware, maybe there's a fix.

CryptoLockers



Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

CryptoLockers / Ransomware encrypts all files on your computer it can find and asks for money.

Don't Panic! Research the malware, maybe there's a fix.

Prevention is the best medicine. Keep your systems up-to-date and have recent external backups.

Anti-Virus

Many of you might never have thought about installing anti-virus software because default defences have improved, but it is still recommended practice.

Anti-Virus

Many of you might never have thought about installing anti-virus software because default defences have improved, but it is still recommended practice.

It's too big a market to make an informed recommendation, but I use Kaspersky (for their focus on Stalkerware).

Anti-Virus

Many of you might never have thought about installing anti-virus software because default defences have improved, but it is still recommended practice.

It's too big a market to make an informed recommendation, but I use Kaspersky (for their focus on Stalkerware).

Anti-Malware Software is not just for your PC or Laptop. Your phone is just as much a computer and probably even more of a target.

Anti-Virus

Many of you might never have thought about installing anti-virus software because default defences have improved, but it is still recommended practice.

It's too big a market to make an informed recommendation, but I use Kaspersky (for their focus on Stalkerware).

Anti-Malware Software is not just for your PC or Laptop. Your phone is just as much a computer and probably even more of a target.
Do not be dissuaded by the mere numerical "Most Android Anti-Malware apps offer no protection".

VPNs

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.

Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network.

VPN Advertisement Claims:

You might have seen an increasing number of adverts for VPNs (e.g. in educational YouTube). Some of it is for real, some of it is snake oil. A quick rundown:

VPN Advertisement Claims:

You might have seen an increasing number of adverts for VPNs (e.g. in educational YouTube). Some of it is for real, some of it is snake oil. A quick rundown:

- **“Everytime you connect to public Wi-Fi, you risk data theft!”**
  Generally not true (anymore). Banned by UK regulators.

VPN Advertisement Claims:

You might have seen an increasing number of adverts for VPNs (e.g. in educational YouTube). Some of it is for real, some of it is snake oil. A quick rundown:

- **“Everytime you connect to public Wi-Fi, you risk data theft!”**
  Generally not true (anymore). Banned by UK regulators.
- **“This VPN uses military-grade encryption!”**
  True, but meaningless.

VPN Advertisement Claims:

You might have seen an increasing number of adverts for VPNs (e.g. in educational YouTube). Some of it is for real, some of it is snake oil. A quick rundown:

- **“Everytime you connect to public Wi-Fi, you risk data theft!”**
  Generally not true (anymore). Banned by UK regulators.
- **“This VPN uses military-grade encryption!”**
  True, but meaningless.
- **“Your ISP can see your metadata!”**
  True, and there are good reasons to hide metadata. But no contents!

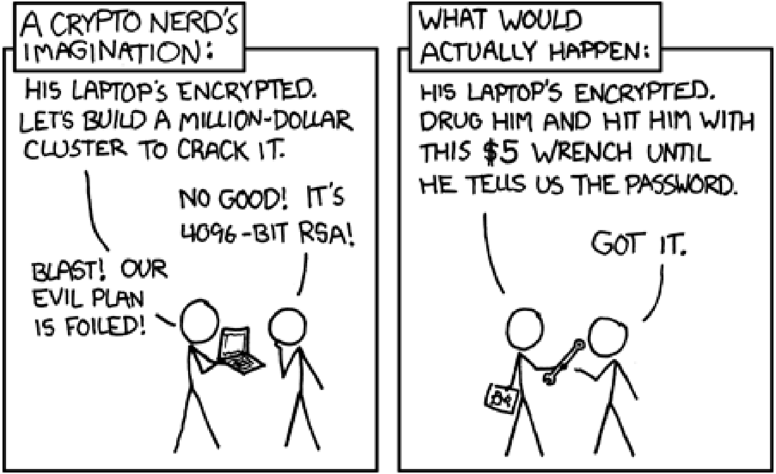
VPN Advertisement Claims:

You might have seen an increasing number of adverts for VPNs (e.g. in educational YouTube). Some of it is for real, some of it is snake oil. A quick rundown:

- **"Everytime you connect to public Wi-Fi, you risk data theft!"**
  Generally not true (anymore). Banned by UK regulators.
- **"This VPN uses military-grade encryption!"**
  True, but meaningless.
- **"Your ISP can see your metadata!"**
  True, and there are good reasons to hide metadata. But no contents!
- **"The VPN doesn't keep logs of your activity!"**
  Potentially true, but indistinguishable from a user perspective.

Social Attacks

No setup gives perfect security!


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Phishing (1)

Phishing (homophone of “fishing”) is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Phishing (1)

Phishing (homophone of “fishing”) is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

Phishing (1)

Phishing (homophone of “fishing”) is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

- Websites can be faked to look exactly like the read deal.

Phishing (1)

Phishing (homophone of “fishing”) is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

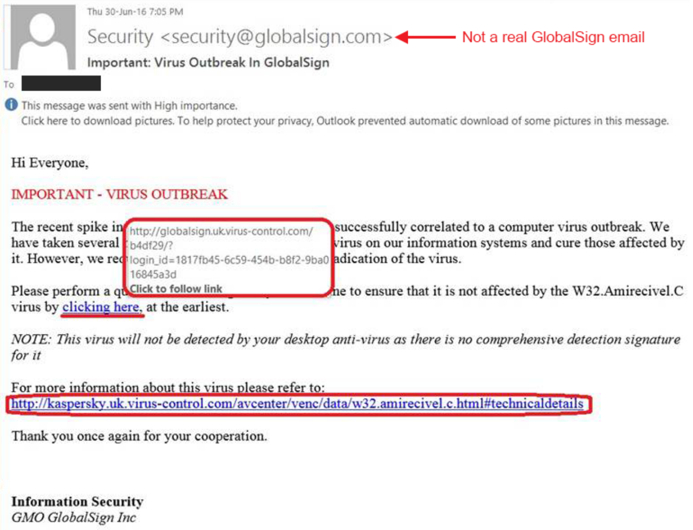
- Websites can be faked to look exactly like the read deal.
- Many Phishers take out fake advertisements.

Phishing (1)

Phishing (homophone of “fishing”) is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

- Websites can be faked to look exactly like the read deal.
- Many Phishers take out fake advertisements.
- Email addresses are *incredibly* easy to fake.

Phishing (2)



Thu 30-Jun-16 7:05 PM

Security <security@globalsign.com>

Not a real GlobalSign email

Important: Virus Outbreak In GlobalSign

To [redacted]

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi Everyone,

IMPORTANT - VIRUS OUTBREAK

The recent spike in successfully correlated to a computer virus outbreak. We have taken several virus on our information systems and cure those affected by it. However, we re adication of the virus.

http://globalsign.ukvirus-control.com/
b4df29/?
login_id=1817fb45-6c59-454b-b8f2-9ba0
16845a3d
Click to follow link

Please perform a q ne to ensure that it is not affected by the W32.Amirecivel.C virus by clicking here, at the earliest.

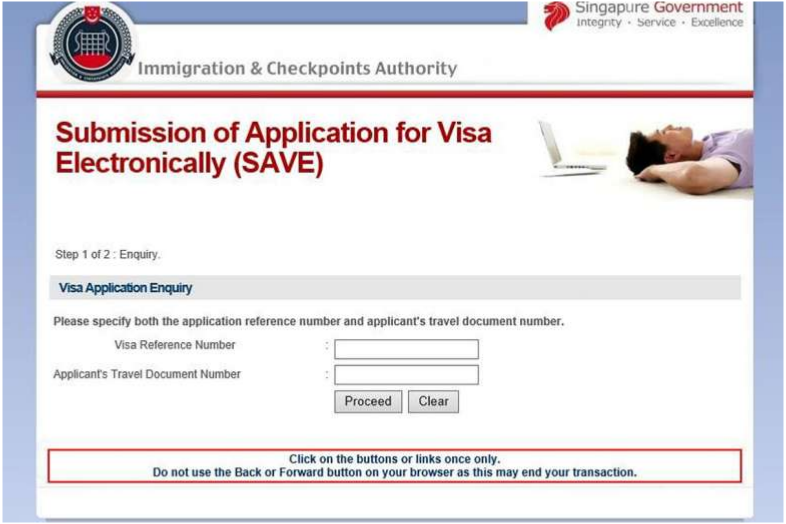
NOTE: This virus will not be detected by your desktop anti-virus as there is no comprehensive detection signature for it

For more information about this virus please refer to:
http://kaspersky.uk.virus-control.com/avcenter/venc/data/w32.amirecivel.c.html#technicaldetails

Thank you once again for your cooperation.

Information Security
GMO GlobalSign Inc

Phishing (3)



Singapore Government
Integrity · Service · Excellence
Immigration & Checkpoints Authority

Submission of Application for Visa Electronically (SAVE)

Step 1 of 2 : Enquiry.

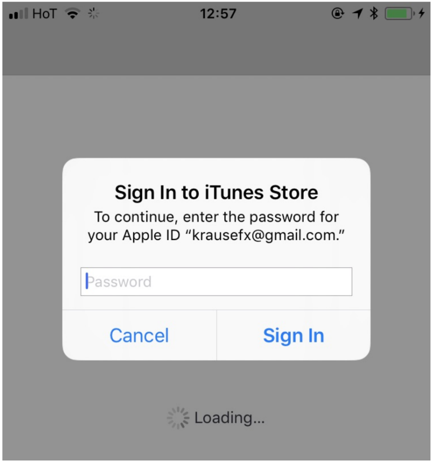
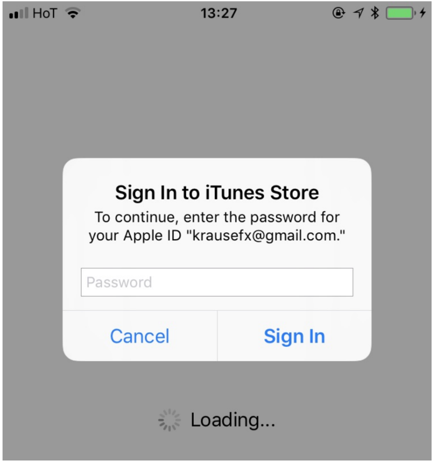
Visa Application Enquiry

Please specify both the application reference number and applicant's travel document number.

Visa Reference Number	:
Applicant's Travel Document Number	:

Click on the buttons or links once only.
Do not use the Back or Forward button on your browser as this may end your transaction.

Phishing (4)

Official popup	Phishing popup
 Sign In to iTunes Store To continue, enter the password for your Apple ID “krausefx@gmail.com.” 	 Sign In to iTunes Store To continue, enter the password for your Apple ID "krausefx@gmail.com."

Social Engineering

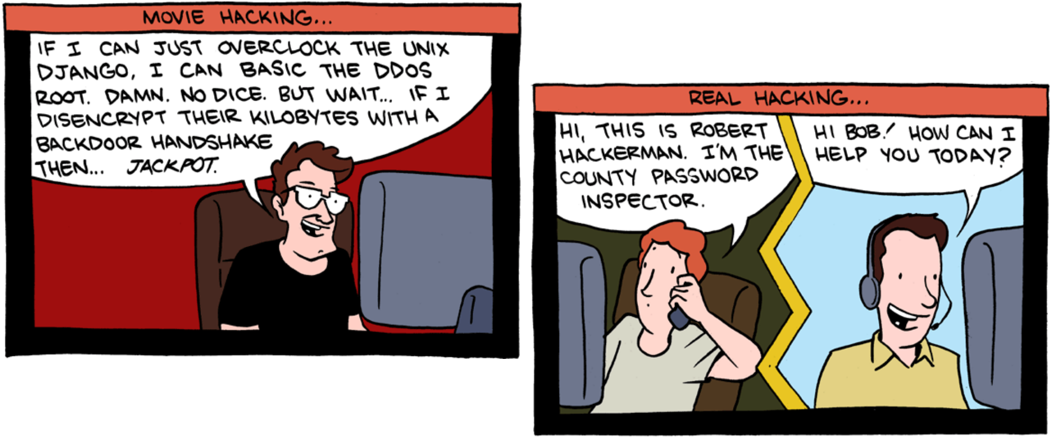
Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. It has also been defined as ”any act that influences a person to take an action that may or may not be in their best interests.”

Social Engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. It has also been defined as ”any act that influences a person to take an action that may or may not be in their best interests.”

Again, an important factor in defending against such attacks is knowledge and training. Practice saying “No” to unreasonable requests.

How it works. . .


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Social Engineering (2)

The six key principles of social engineering:

Social Engineering (2)

The six key principles of social engineering:

- **Reciprocity**
  People tend to return favours given to them, even if they didn't ask for them.

Social Engineering (2)

The six key principles of social engineering:

- **Reciprocity**
  People tend to return favours given to them, even if they didn't ask for them.
- **Commitment**
  People tend to keep promises, even if the original incentive is removed.

Social Engineering (2)

The six key principles of social engineering:

- **Reciprocity**
  People tend to return favours given to them, even if they didn't ask for them.
- **Commitment**
  People tend to keep promises, even if the original incentive is removed.
- **Conformity**
  People tend to do what they see other people doing (see Asch).

Social Engineering (2)

The six key principles of social engineering:

- **Reciprocity**
  People tend to return favours given to them, even if they didn't ask for them.
- **Commitment**
  People tend to keep promises, even if the original incentive is removed.
- **Conformity**
  People tend to do what they see other people doing (see Asch).
- **Authority**
  People tend to obey authority figures (see Milgram).

Social Engineering (2)

The six key principles of social engineering:

- **Reciprocity**
  People tend to return favours given to them, even if they didn't ask for them.
- **Commitment**
  People tend to keep promises, even if the original incentive is removed.
- **Conformity**
  People tend to do what they see other people doing (see Asch).
- **Authority**
  People tend to obey authority figures (see Milgram).
- **Liking**
  People are more easily persuaded by people they like (Tupperware, MLMs).

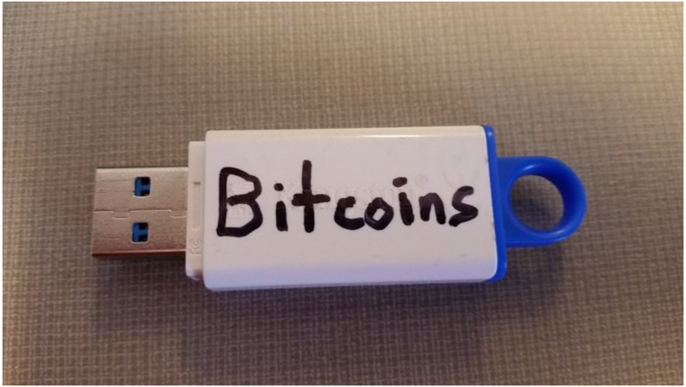
Social Engineering (2)

The six key principles of social engineering:

- **Reciprocity**
  People tend to return favours given to them, even if they didn't ask for them.
- **Commitment**
  People tend to keep promises, even if the original incentive is removed.
- **Conformity**
  People tend to do what they see other people doing (see Asch).
- **Authority**
  People tend to obey authority figures (see Milgram).
- **Liking**
  People are more easily persuaded by people they like (Tupperware, MLMs).
- **Scarcity**
  Perceived scarcity will generate demand ("Limited Time Only").

But also: *Urgency, Curiosity, . . .*

Social Engineering (3))



Social Engineering (4)

(video with Rachel Tobac)

Social Engineers

Coordinate with one or more partners from around the room, exchange names and – given that you have their consent – with the search engine of your choice, try and find out some personal information about them or yourself that could be used to either find more information or wrongly authenticate yourself as them in front of third parties.

If any of you feel uncomfortable with this exercise, that is absolutely okay. Nobody has to participate if they do not wish it. If your group has no volunteers, take me instead (my full name, again, is "Jonas Betzendahl").

Miscellaneous

Internet of Things

Over the past few years, more and more internet-enabled devices (voice assistants, doors, toasters, even dolls!) have moved into “smart homes” and offices.

Internet of Things

Over the past few years, more and more internet-enabled devices (voice assistants, doors, toasters, even dolls!) have moved into “smart homes” and offices.

The companies behind these products often have poor standards of operational security and data safety.

Internet of Things

Over the past few years, more and more internet-enabled devices (voice assistants, doors, toasters, even dolls!) have moved into “smart homes” and offices.

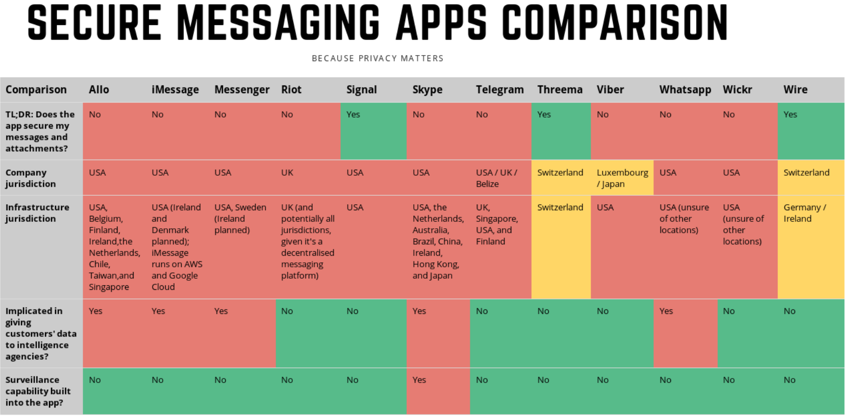
The companies behind these products often have poor standards of operational security and data safety.

There is little to say besides “Don’t get one.”, but if you do, research the device beforehand and make sure that firmware is up-to-date and default credentials are changed.

Secure Messaging Apps (1)

Secure Messaging Apps (2)

More detailed overview: `https://www.securemessagingapps.com/`



SECURE MESSAGING APPS COMPARISON

BECAUSE PRIVACY MATTERS

Comparison	Allo	iMessage	Messenger	Riot	Signal	Skype	Telegram	Threema	Viber	Whatsapp	Wickr	Wire
TL;DR: Does the app secure my messages and attachments?	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes
Company jurisdiction	USA	USA	USA	UK	USA	USA	USA / UK / Belize	Switzerland	Luxembourg / Japan	USA	USA	Switzerland
Infrastructure jurisdiction	USA, Belgium, Finland, Ireland,the Netherlands, Chile, Taiwan,and Singapore	USA (Ireland and Denmark planned); iMessage runs on AWS and Google Cloud	USA, Sweden (Ireland planned)	UK (and potentially all jurisdictions, given it's a decentralised messaging platform)	USA	USA, the Netherlands, Australia, Brazil, China, Ireland, Hong Kong, and Japan	UK, Singapore, USA, and Finland	Switzerland	USA	USA (unsure of other locations)	USA (unsure of other locations)	Germany / Ireland
Implicated in giving customers' data to intelligence agencies?	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	No
Surveillance capability built into the app?	No	No	No	No	No	Yes	No	No	No	No	No	No

2FA

Multi-factor authentication (MFA) 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:

- knowledge (something the user and only the user knows)
- possession (something the user and only the user has)
- inherence (something the user and only the user is)

2FA

Multi-factor authentication (MFA) 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:

- knowledge (something the user and only the user knows)
- possession (something the user and only the user has)
- inherence (something the user and only the user is)

This is already in place with ATMs, but can also used for many online platforms via smartphone. This has advantages and drawbacks but is generally considered positive.

Advanced 2FA

Having more security in place is almost universally a good thing. You want to be as difficult a target as you can be. But even 2FA does not provide universal protection.

Advanced 2FA

Having more security in place is almost universally a good thing. You want to be as difficult a target as you can be. But even 2FA does not provide universal protection.

This is especially true if your second factor is your phone number. Phone number / name combinations are often included in big data leaks and allow for *SIM swapping*.

Advanced 2FA

Having more security in place is almost universally a good thing. You want to be as difficult a target as you can be. But even 2FA does not provide universal protection.

This is especially true if your second factor is your phone number. Phone number / name combinations are often included in big data leaks and allow for *SIM swapping*.

There are other possibilities for 2FA/MFA, even specialised devices such as a *Yubikey*.

Fake News

There are multiple outlets online that, for one reason or another (political gain, satire, "for teh lulz", . . .) will deliberately spread false information, often with false evidence attached (e.g. doctored images).

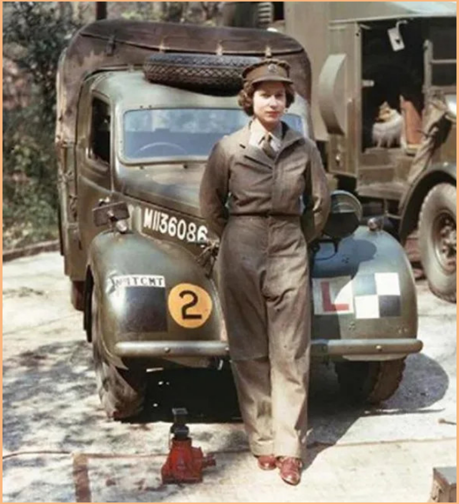
Fake News

There are multiple outlets online that, for one reason or another (political gain, satire, “for teh lulz”, . . .) will deliberately spread false information, often with false evidence attached (e.g. doctored images).

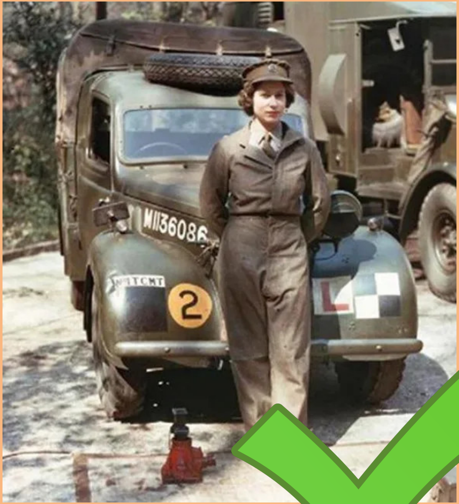
Be aware that this is happening. A good habit to have is verifying / fact checking important information before acting on it. There are even dedicated fact checking journalism outlets that respond to popular content:

- English: `https://www.snopes.com`
- German: `https://correctiv.org/faktencheck/`

Fake News Quiz (1)

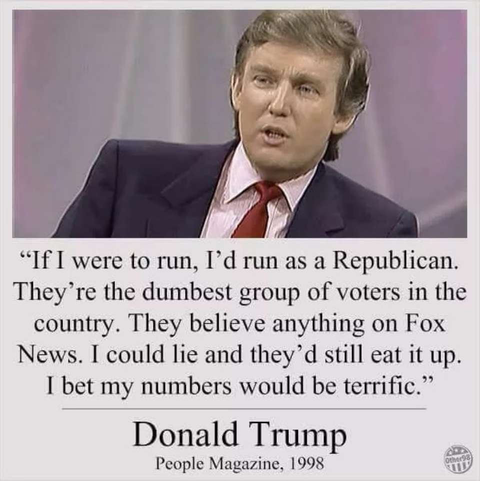


Fake News Quiz (1)



✓

Fake News Quiz (2)

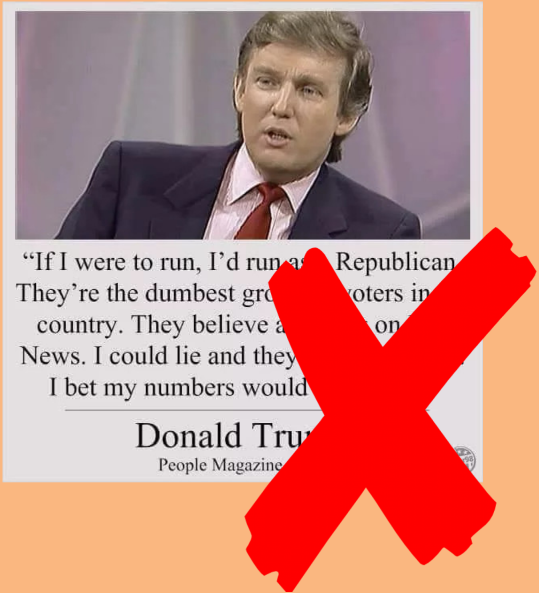


“If I were to run, I’d run as a Republican. They’re the dumbest group of voters in the country. They believe anything on Fox News. I could lie and they’d still eat it up. I bet my numbers would be terrific.”

Donald Trump

People Magazine, 1998

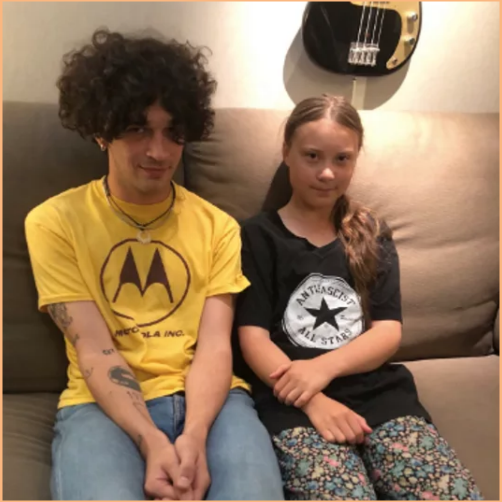
Fake News Quiz (2)



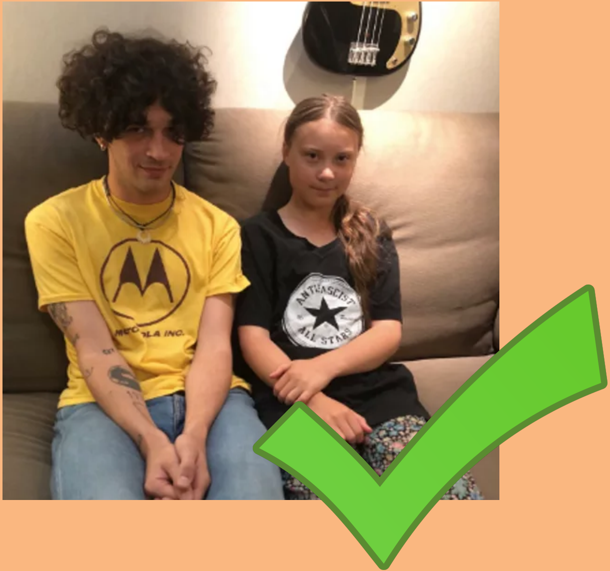
“If I were to run, I’d run as Republican
They’re the dumbest gro voters in
country. They believe a on
News. I could lie and they
I bet my numbers would

Donald Tru
People Magazine

Fake News Quiz (3)

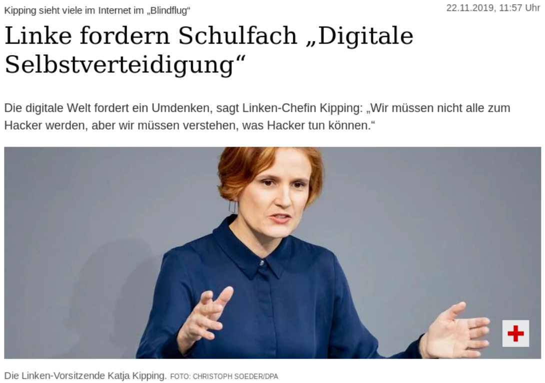


Fake News Quiz (3)



Conclusion

In the long run. . .



Kipping sieht viele im Internet im „Blindflug“

22.11.2019, 11:57 Uhr

Linke fordern Schulfach „Digitale Selbstverteidigung“

Die digitale Welt fordert ein Umdenken, sagt Linken-Chefin Kipping: „Wir müssen nicht alle zum Hacker werden, aber wir müssen verstehen, was Hacker tun können.“

Die Linken-Vorsitzende Katja Kipping. FOTO: CHRISTOPH SOEDER/DPA

Learn & Teach

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**
- **. . . check for identity leaks.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**
- **. . . check for identity leaks.**
- **. . . get a secure (end-to-end) messenger.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**
- **. . . check for identity leaks.**
- **. . . get a secure (end-to-end) messenger.**
- **. . . review apps & permissions on your phone.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**
- **. . . check for identity leaks.**
- **. . . get a secure (end-to-end) messenger.**
- **. . . review apps & permissions on your phone.**
- **. . . install newest software updates.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**
- **. . . check for identity leaks.**
- **. . . get a secure (end-to-end) messenger.**
- **. . . review apps & permissions on your phone.**
- **. . . install newest software updates.**
- **. . . install anti-virus software.**

Things you can do this weekend:

The best things to keep in mind are the things that you can do soon:

- **. . . install/change lockscreen PIN.**
- **. . . get a password manager.**
- **. . . check for identity leaks.**
- **. . . get a secure (end-to-end) messenger.**
- **. . . review apps & permissions on your phone.**
- **. . . install newest software updates.**
- **. . . install anti-virus software.**
- **. . . enable 2FA where applicable.**

Resources

- *Surveillance Self-Defence* @ EFF, `https://ssd.eff.org`
- *Coalition against Stalkerware*, `https://stopstalkerware.org/`
- *Secure Messaging Apps*, `https://www.securemessagingapps.com/`
- *Identity Leak Checker* @ HPI, `https://sec.hpi.de/ilc/`
- Initiative *Aktiv gegen Digitale Gewalt*, `https://www.aktiv-gegen-digitale-gewalt.de`
- Initiative *Frauen gegen Gewalt*, `https://frauen-gegen-gewalt.de`
- Comparison of *password managers* @ Wikipedia, `https://en.wikipedia.org/wiki/List_of_password_managers`

Sources

- *Watch a CNN reporter get hacked!*: `https://www.youtube.com/watch?v=yIG4kTJTZuY`
- Wired, *Don't Rely On an Unlock Pattern To Secure Your Android Phone*: `https://www.wired.com/story/android-unlock-pattern-or-pin/`
- UK Advertisement Regulatory Ruling Re: NordVPN: `https://www.asa.org.uk/rulings/tefincom-sa-a19-547668.html`
- Tom Scott's "This Video Is Sponsored By [redacted] VPN": `https://www.youtube.com/watch?v=WVDQEoe6ZWY`
- ExtremeTech's *"Most Android Anti-Malware Apps Don't Offer Any Protection"* `https://www.extremetech.com/mobile/287790-most-android-anti-malware-apps-dont-offer-any-protection`
- Reply All's *The Snapchat Thief*: `https://gimletmedia.com/shows/reply-all/v4he6k`