Computers and Cyber Security

Next Generation Programmers
8th June 2021
Dr Matthew Bradbury

Who am I?

Matthew Bradbury

- Enjoy cycling (especially in the rain)
- Collect bronze frogs
- Have big family get togethers
- My music tastes haven’t changed much from when I was 20

I work at Lancaster University

Lecturer in Cyber Security at Lancaster University

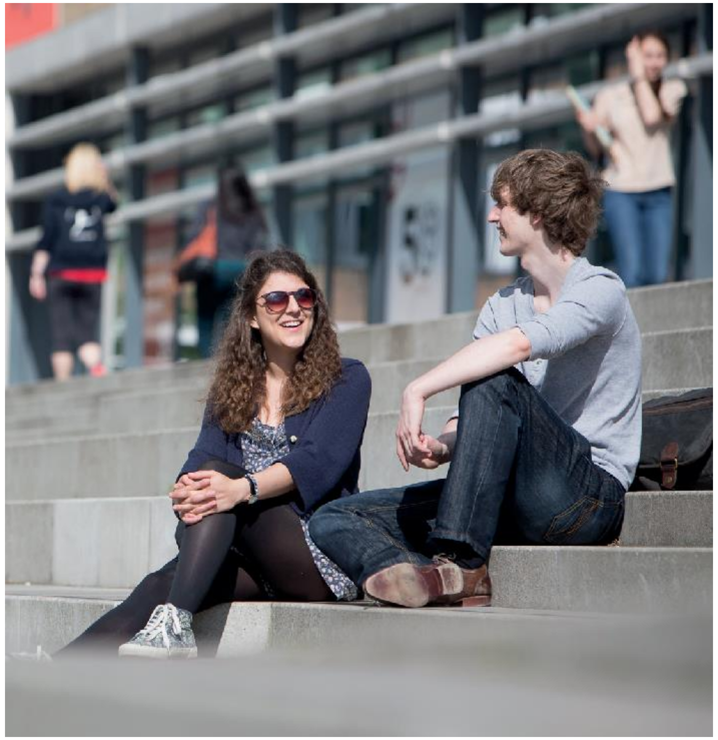
Edinburgh

Lancaster

Birmingham

London

Lots of nice spots on campus



Lancaster University

What do you think I do?

Find ingenious ways to secure Internet-of-Things (IoT) networks from attackers

Numerous applications, for example:

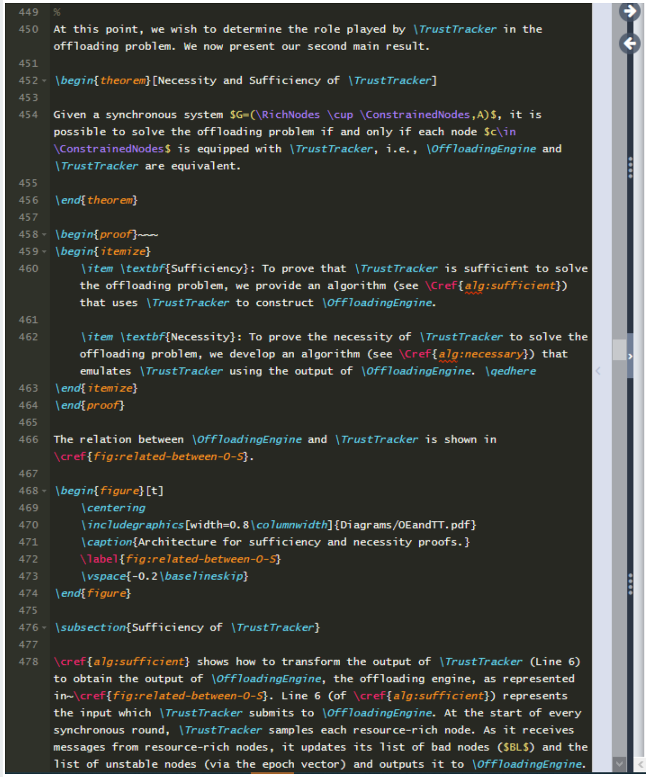
- Allowing Scientists to track pandas using sensors
- While also not allowing poachers to use the same sensors to find pandas

Photo by @Amivee taken at the Wolong National Nature Reserve

This is what I do!

🤔 ❓ 💡 ❗

Some of this… (developing new theory)



```
%
At this point, we wish to determine the role played by \TrustTracker in the
offloading problem. We now present our second main result.

\begin{theorem}[Necessity and Sufficiency of \TrustTracker]

Given a synchronous system $G=(\RichNodes \cup \ConstrainedNodes,A)$, it is
possible to solve the offloading problem if and only if each node $c\in
\ConstrainedNodes$ is equipped with \TrustTracker, i.e., \OffloadingEngine and
\TrustTracker are equivalent.

\end{theorem}

\begin{proof}~~~
\begin{itemize}
    \item \textbf{Sufficiency}: To prove that \TrustTracker is sufficient to solve
    the offloading problem, we provide an algorithm (see \Cref{alg:sufficient})
    that uses \TrustTracker to construct \OffloadingEngine.

    \item \textbf{Necessity}: To prove the necessity of \TrustTracker to solve the
    offloading problem, we develop an algorithm (see \Cref{alg:necessary}) that
    emulates \TrustTracker using the output of \OffloadingEngine. \qedhere
\end{itemize}
\end{proof}

The relation between \OffloadingEngine and \TrustTracker is shown in
\cref{fig:related-between-O-S}.

\begin{figure}[t]
    \centering
    \includegraphics[width=0.8\columnwidth]{Diagrams/OEandTT.pdf}
    \caption{Architecture for sufficiency and necessity proofs.}
    \label{fig:related-between-O-S}
    \vspace{-0.2\baselineskip}
\end{figure}

\subsection{Sufficiency of \TrustTracker}

\cref{alg:sufficient} shows how to transform the output of \TrustTracker (Line 6)
to obtain the output of \OffloadingEngine, the offloading engine, as represented
in~\cref{fig:related-between-O-S}. Line 6 (of \cref{alg:sufficient}) represents
the input which \TrustTracker submits to \OffloadingEngine. At the start of every
synchronous round, \TrustTracker samples each resource-rich node. As it receives
messages from resource-rich nodes, it updates its list of bad nodes ($BL$) and the
list of unstable nodes (via the epoch vector) and outputs it to \OffloadingEngine.
```

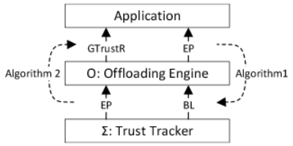


Figure 1: Architecture for sufficiency and necessity proofs.

The completeness property of the trust detector captures issues caused by untrusted nodes (i.e., bad and unstable nodes). It associates edge nodes with an epoch number to detect unstable nodes. On the other hand, the accuracy property stipulates that (eventually) good nodes are permanently trusted. We denote the trust tracker device by Σ. At this point, we wish to determine the role played by Σ in the offloading problem. We now present our second main result.

Theorem 2 (Necessity and Sufficiency of Σ). *Given a synchronous system $G = (V_R \cup V_C, A)$, it is possible to solve the offloading problem if and only if each node $c \in V_C$ is equipped with Σ, i.e., $\mathcal{O}$ and Σ are equivalent.*

Proof.

- **Sufficiency**: To prove that Σ is sufficient to solve the offloading problem, we provide an algorithm (see Algorithm 1) that uses Σ to construct $\mathcal{O}$.
- **Necessity**: To prove the necessity of Σ to solve the offloading problem, we develop an algorithm (see Algorithm 2) that emulates Σ using the output of $\mathcal{O}$. □

The relation between $\mathcal{O}$ and Σ is shown in Figure 1.

A. Sufficiency of Σ

Algorithm 1 shows how to transform the output of Σ (Line 6) to obtain the output of $\mathcal{O}$, the offloading engine, as represented in Figure 1. Line 6 (of Algorithm 1) represents the input which Σ submits to $\mathcal{O}$. At the start of every synchronous round, Σ samples each resource-rich node. As it receives messages from resource-rich nodes, it updates its list of bad nodes (BL) and the list of unstable nodes (via the epoch vector) and outputs it to $\mathcal{O}$. We assume a threshold σ to identify unstable nodes. When $\mathcal{O}$ is ready to select an edge node for offloading, Σ outputs the list $GtrustR$ of trusted nodes (those that are good

Algorithm 1 Sufficiency: Σ sufficient to solve $\mathcal{O}$

```
    ▷ Output of Σ to obtain offloading engine
1:  function INIT
2:      START($off, \delta$)                                  ▷ Timer
3:      $Ep \leftarrow V_R \times \{0\}$                      ▷ $Ep \in V_R \rightarrow \mathbb{N}_0$
        ▷ Trusted nodes in one round
4:      $trustR \leftarrow V_R$                               ▷ $trustR \in 2^{V_R}$
        ▷ Those identified as trusted over multiple rounds
5:      $GtrustR \leftarrow V_R$                              ▷ $GtrustR \in 2^{V_R}$
6:  event EVALUATED($BL, E$) → ▷ $BL$: bad list, $E$: Epoch
7:      $Ep, trustR \leftarrow E, V_R$                        ▷ Reset
8:      $UR \leftarrow \{u \mid u \in V_R \wedge E(u) \geq \sigma\}$   ▷ Unstable nodes
9:      $trustR \leftarrow trustR \setminus BL$               ▷ Remove bad nodes
10:     $trustR \leftarrow trustR \setminus UR$               ▷ Remove unstable nodes
        ▷ Nodes that are permanently good
11:     $GtrustR \leftarrow GtrustR \cap trustR$
12: timeout ($off$) →                                          ▷ Offloading decision time
13:     if $GtrustR \neq \emptyset$ then
14:         return ($GtrustR, Ep$)
15:     else
16:         START($off, \delta$)
17:         $GtrustR \leftarrow trustR$
```

Algorithm 2 Necessity: Σ necessary to solve $\mathcal{O}$

```
    ▷ Output of offloading engine to obtain Σ
1:  function OUTPUT($T_r, E$)
2:      $UR \leftarrow \{u \mid u \in V_R \wedge E(u) \geq \sigma\}$
3:      $BL \leftarrow V_R \setminus (UR \cup T_r)$
4:      return ($BL, E$)
```

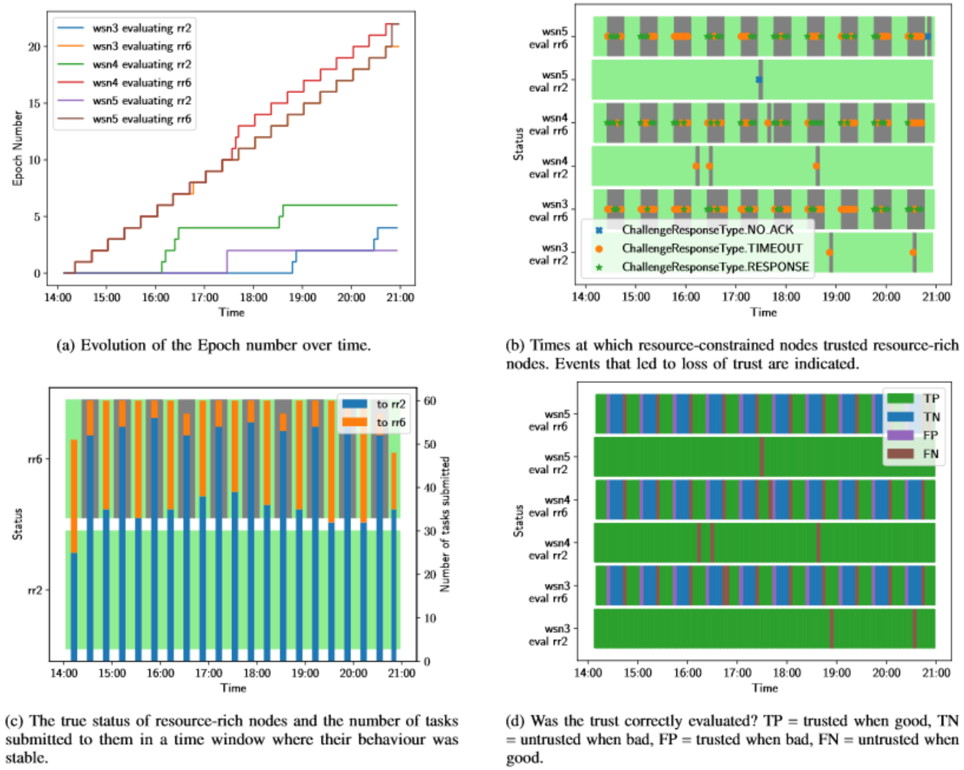
VI. Implementing Σ and Probabilistic Offloading

The use of Σ makes it possible to solve the offloading problem, however, it still needs to be understood if it is possible to implement Σ in a synchronous system. Unfortunately, the answer is negative. Our third major result is thus:

Theorem 3 (Impossibility of implementing Σ). *Given a synchronous system, it is impossible to implement Σ.*

Proof. We assume an algorithm $\mathcal{A}$ exists for Σ and then show a contradiction.

Consider a failure pattern $\mathcal{F}_0$ where there are no failures and consider a computation



(a) Evolution of the Epoch number over time.

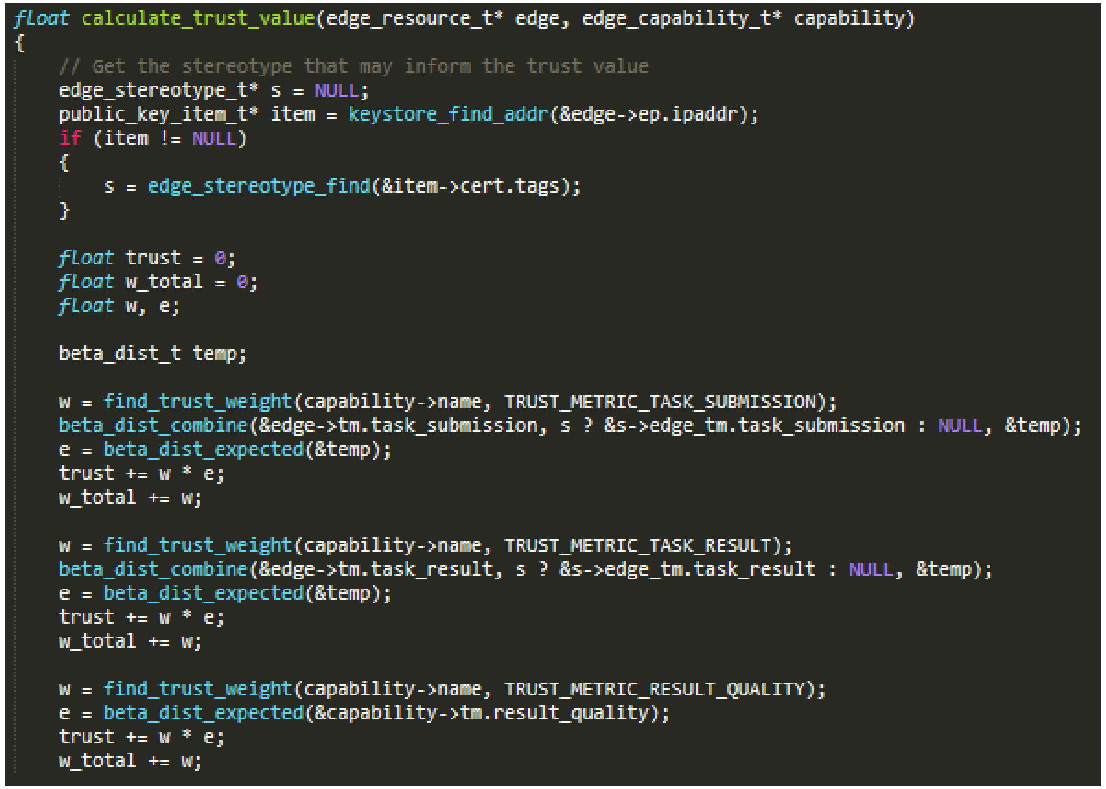
(b) Times at which resource-constrained nodes trusted resource-rich nodes. Events that led to loss of trust are indicated.

(c) The true status of resource-rich nodes and the number of tasks submitted to them in a time window where their behaviour was stable.

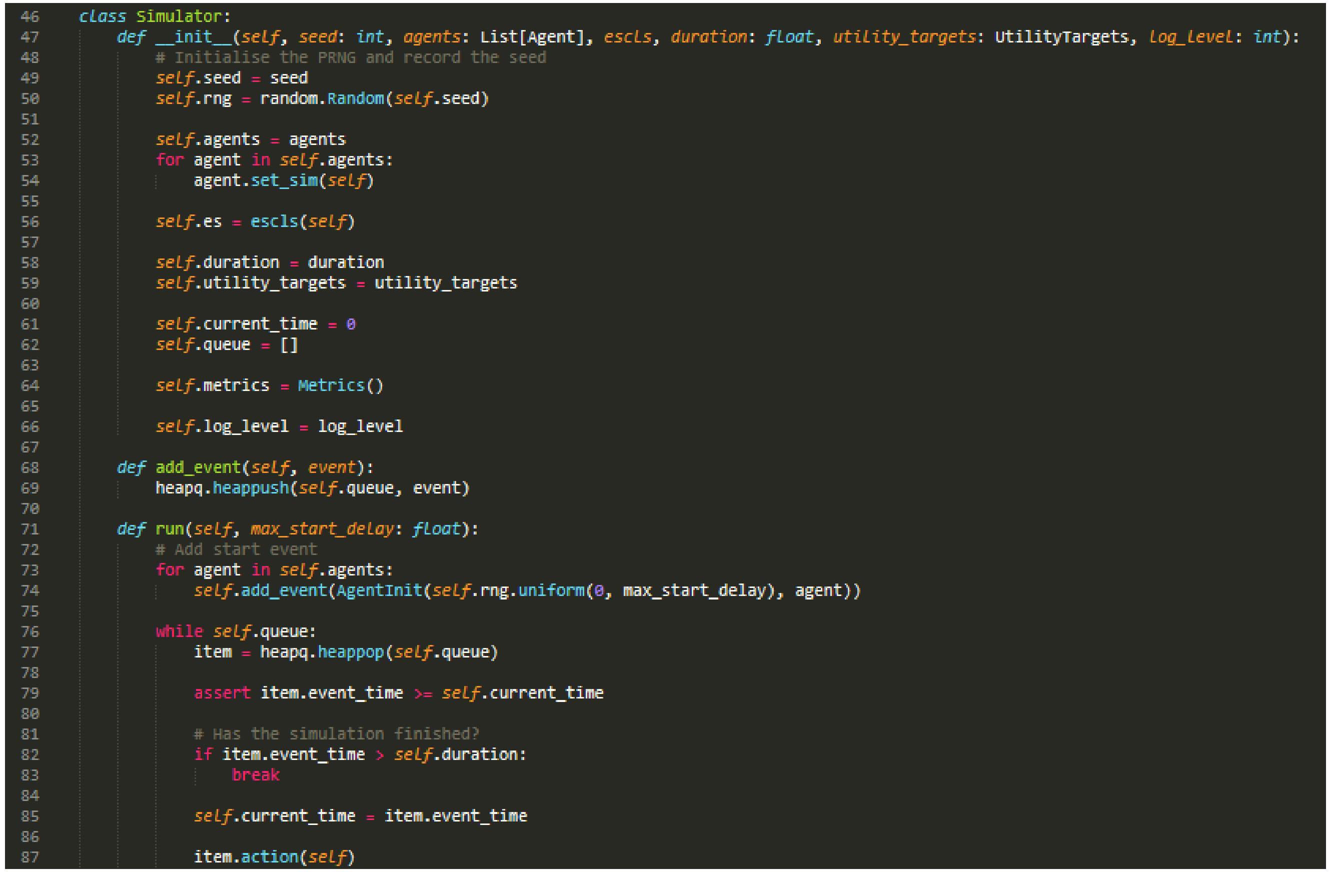
(d) Was the trust correctly evaluated? TP = trusted when good, TN = untrusted when bad, FP = trusted when bad, FN = untrusted when good.

Figure 6: Results for when resource-rich node 2 is good and 6 is unstable.

And this… (writing code!)



```c
float calculate_trust_value(edge_resource_t* edge, edge_capability_t* capability)
{
    // Get the stereotype that may inform the trust value
    edge_stereotype_t* s = NULL;
    public_key_item_t* item = keystore_find_addr(&edge->ep.ipaddr);
    if (item != NULL)
    {
        s = edge_stereotype_find(&item->cert.tags);
    }

    float trust = 0;
    float w_total = 0;
    float w, e;

    beta_dist_t temp;

    w = find_trust_weight(capability->name, TRUST_METRIC_TASK_SUBMISSION);
    beta_dist_combine(&edge->tm.task_submission, s ? &s->edge_tm.task_submission : NULL, &temp);
    e = beta_dist_expected(&temp);
    trust += w * e;
    w_total += w;

    w = find_trust_weight(capability->name, TRUST_METRIC_TASK_RESULT);
    beta_dist_combine(&edge->tm.task_result, s ? &s->edge_tm.task_result : NULL, &temp);
    e = beta_dist_expected(&temp);
    trust += w * e;
    w_total += w;

    w = find_trust_weight(capability->name, TRUST_METRIC_RESULT_QUALITY);
    e = beta_dist_expected(&capability->tm.result_quality);
    trust += w * e;
    w_total += w;
```

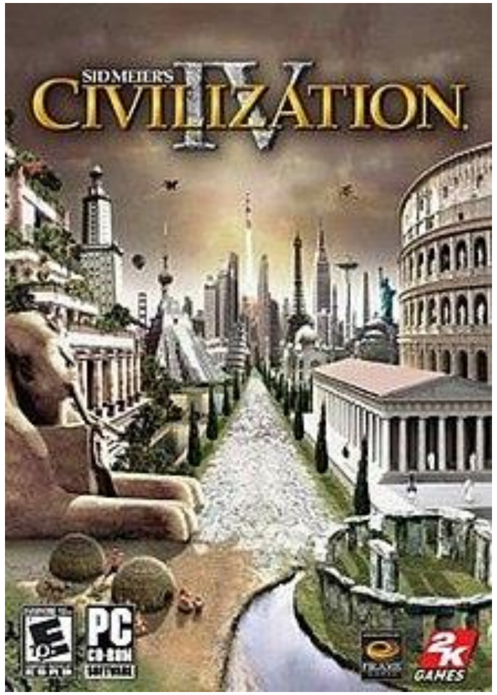


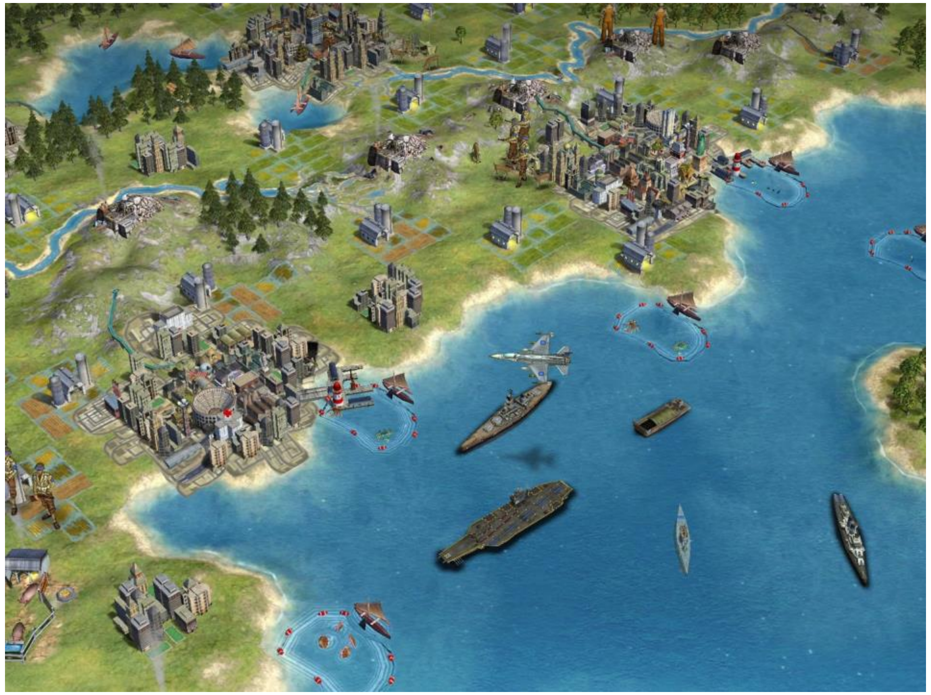
```python
class Simulator:
    def __init__(self, seed: int, agents: List[Agent], escls, duration: float, utility_targets: UtilityTargets, log_level: int):
        # Initialise the PRNG and record the seed
        self.seed = seed
        self.rng = random.Random(self.seed)

        self.agents = agents
        for agent in self.agents:
            agent.set_sim(self)

        self.es = escls(self)

        self.duration = duration
        self.utility_targets = utility_targets

        self.current_time = 0
        self.queue = []

        self.metrics = Metrics()

        self.log_level = log_level

    def add_event(self, event):
        heapq.heappush(self.queue, event)

    def run(self, max_start_delay: float):
        # Add start event
        for agent in self.agents:
            self.add_event(AgentInit(self.rng.uniform(0, max_start_delay), agent))

        while self.queue:
            item = heapq.heappop(self.queue)

            assert item.event_time >= self.current_time

            # Has the simulation finished?
            if item.event_time > self.duration:
                break

            self.current_time = item.event_time

            item.action(self)
```

But also lots of this!
(experimentation and talks)

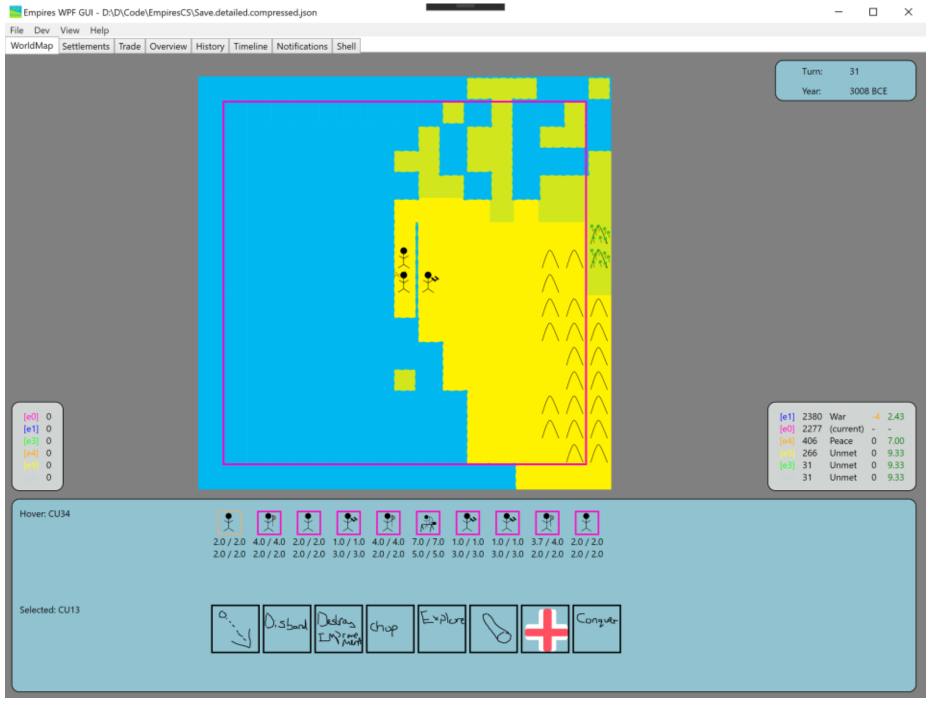
WPCCS 2017
Programme
Security Minded Verification & Validation for Future Space Systems via Reference Architectures
Matthew Bradbury
Cyber Security Centre, WMG, University of Warwick
6th June 2019
WMG
FAIR-SPACE
Li ion 053048
3.7V 800mAh
Formal Verification Properties

How did I get into writing code?





Actual game (much better looking)



Turn: 31
Year: 3008 BCE

```
[e0]  0
[e1]  0
[e3]  0
[e4]  0
[e5]  0
[e2]  0
```

```
[e1]  2380  War        -4  2.43
[e0]  2277  (current)  -   -
[e4]  406   Peace      0   7.00
[e5]  266   Unmet      0   9.33
[e3]  31    Unmet      0   9.33
[e2]  31    Unmet      0   9.33
```

Hover: CU34

```
2.0 / 2.0  4.0 / 4.0  2.0 / 2.0  1.0 / 1.0  4.0 / 4.0  7.0 / 7.0  1.0 / 1.0  1.0 / 1.0  3.7 / 4.0  2.0 / 2.0
2.0 / 2.0  2.0 / 2.0  2.0 / 2.0  3.0 / 3.0  2.0 / 2.0  5.0 / 5.0  3.0 / 3.0  3.0 / 3.0  2.0 / 2.0  2.0 / 2.0
```

Selected: CU13

My attempt (not great)

What interests you about writing code?

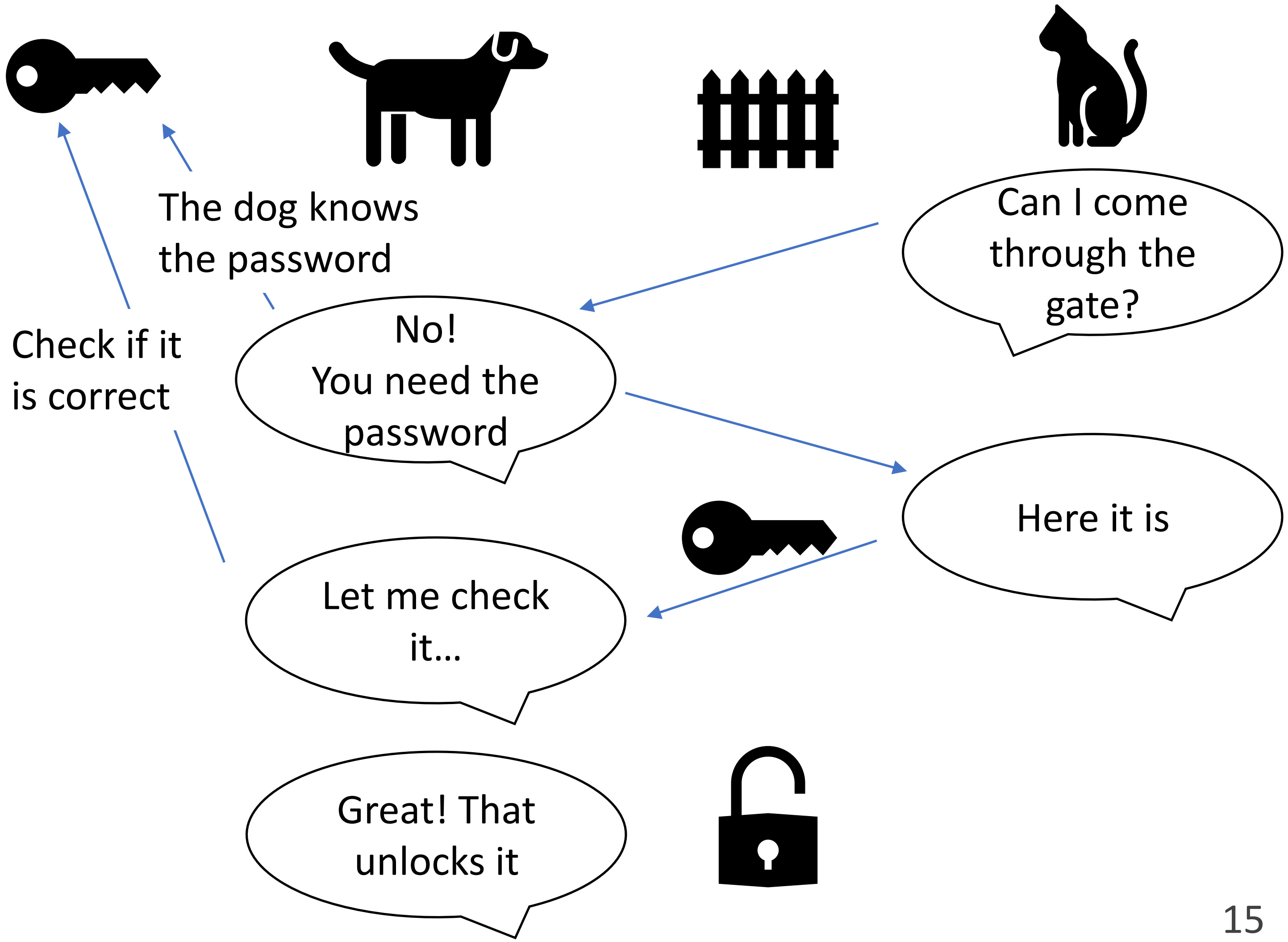
What are we going to look at in this session

Agenda

- How to make a secure password
- The value of your information
- Recognising spam and email manipulation
- Alternatives to pirated software
- The worldwide usefulness of computer and cyber security skills

What is a password, why do we use them?

- Not everyone in the world should have the same access to a system
- Passwords are one approach to limiting who can login to a computer system
- A password is a shared secret



The dog knows the password

Check if it is correct

Can I come through the gate?

No! You need the password

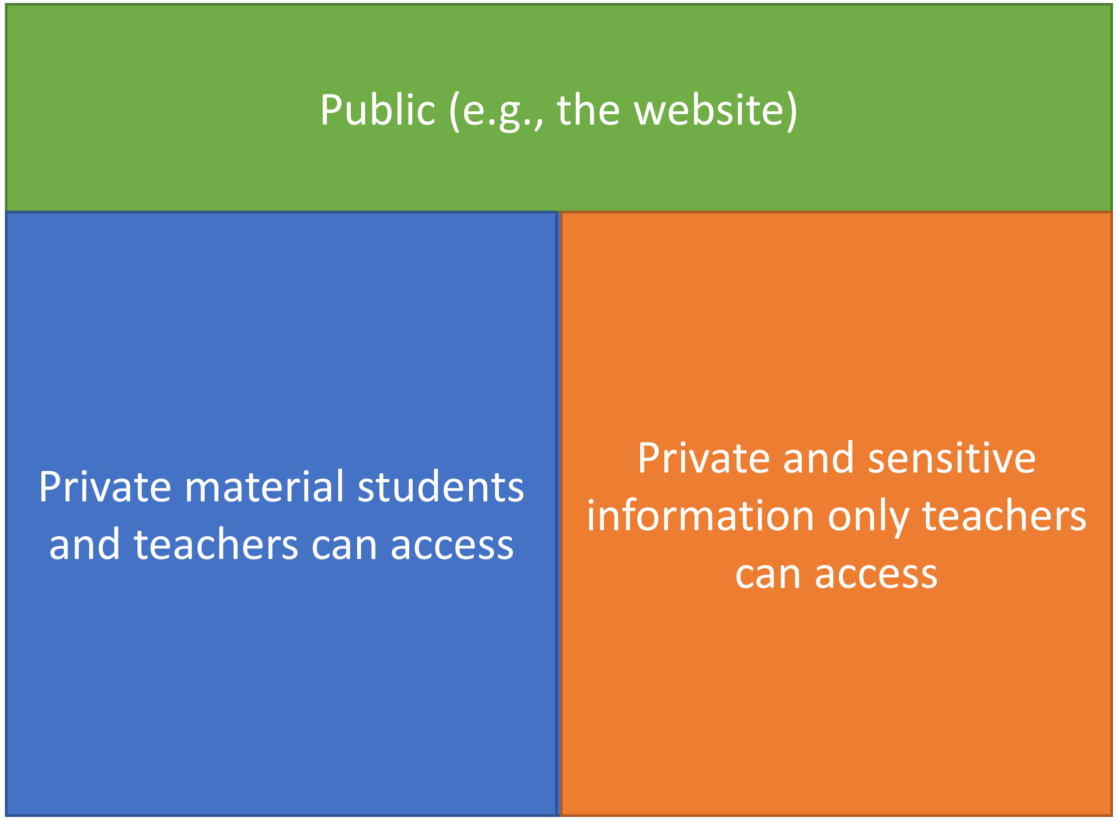
Here it is

Let me check it…

Great! That unlocks it

Not all passwords allow access to everything

- Not everyone should have the same access to a system
- Restrict access to parts of a system that you should not have access to
- Allow access to parts of a system that you should have access to
- **Authentication** – the process of verifying that you are who you claim to be



Public (e.g., the website)

Private material students and teachers can access

Private and sensitive information only teachers can access

What do you think makes a good password?

Don’t share a good password you have!

How can passwords be broken?

- Computers can quickly try many combinations to see what works

Password “abc”:

1. Try “a”, try “b”, …, try “z”
2. Try “aa”, try “ab”, …, try “az”
3. Try “aaa”, try “aab”, …, try “aaz”
4. Try “aba”, try “abb”, try “abc”
5. Found it!

Demo: Coding this!

- Computers can also use dictionaries of common passwords to quickly guess likely options

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678

(source: https://nordpass.com/most-common-passwords-list/)

Demo: Coding a password cracker

Before the demo

- Important to understand how to use these skills ethically
- Do not cause harm to others
- We will discuss ethics in more detail in session 3

How can passwords be broken - Example

- Harder to guess password when:
  - Longer
  - Has numbers and characters
  - Not words found in a dictionary
- Also, passwords could be poorly stored on websites and then leaked if their information is stolen

Demo:
John the Ripper
https://www.openwall.com/john/

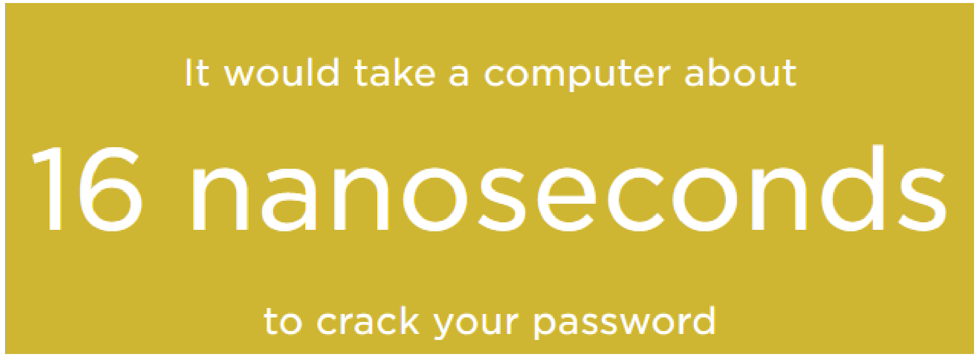
Ethics:

- Use this tool to test effectiveness of passwords
- It is not to be used to break into other systems

Tools to check how strong your passwords are

- https://www.security.org/how-secure-is-my-password/

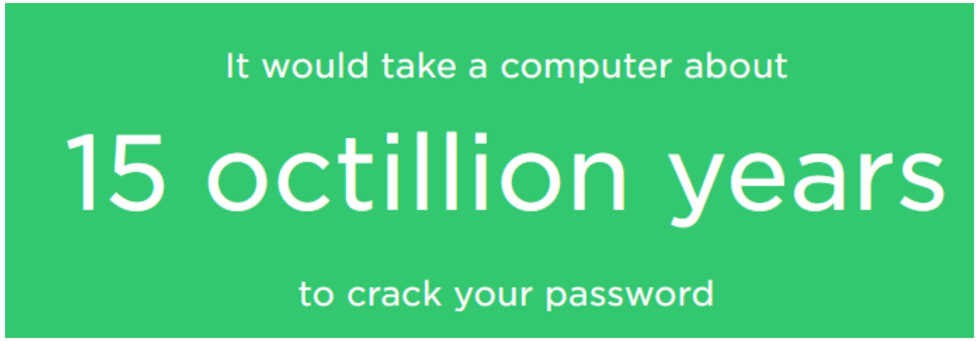
- Never enter your actual passwords into any of these websites
- These websites can easily be used to harvest passwords



It would take a computer about

16 nanoseconds

to crack your password



It would take a computer about

15 octillion years

to crack your password

Password Recommendations (before)

- Make them unique and memorable
- Do not reuse passwords on different websites
- Make passwords long (at least 8 characters)
- Include numbers and special characters !?@:{}
- Avoid common words
- Try to change passwords regularly

Password Recommendations (now)

NIST:

- Make passwords long

https://pages.nist.gov/800-63-3/sp800-63b.html

My advice:

- Try to make passwords at least 12 characters long

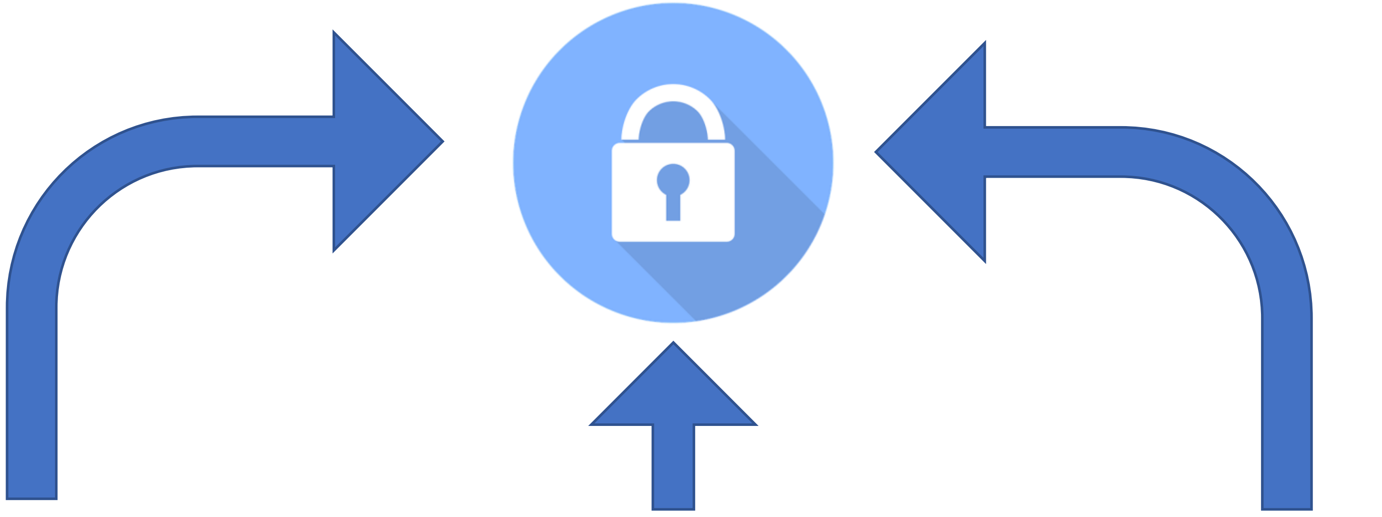
Password Managers

- An even better solution
- Use a password manager
  - Lastpass
  - 1Password
  - KeePassXC (free)
- They generate passwords that are hard for computers to crack
- It is better to use a password manager, as these passwords are harder for humans to remember

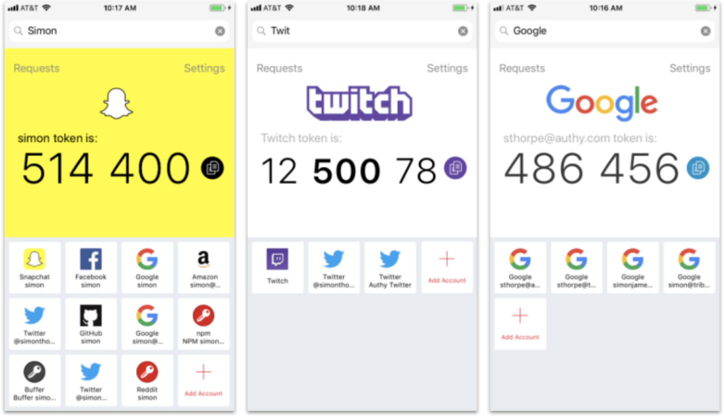
	Easy to remember	Hard to remember
Easy for a computer to crack	• password • aaaaaaaa • p@ssw0rd	• Xr7@#
Harder for a computer to crack	• correcthorse~web site:batterystaple	• KjSpdJPsbX9xeG2 • u4@#1G!7sk;sb& dh&HblVg!7BDsl*

Multi-factor Authentication

- Don’t just rely on passwords
  (a secret you **know**)
- Also:
  - Something you **have**
    (via two factor authentication)
  - Something you **are**
    (biometrics)



Password:
****



AT&T 10:17 AM

Simon

Requests Settings

simon token is:

514 400

Snapchat simon | Facebook simon | Google simon | Amazon simon@...
Twitter @simontho... | GitHub simon | Google simon@... | npm NPM simon...
Buffer Buffer simo... | Twitter @simon... | Reddit simon | Add Account

AT&T 10:18 AM

Twit

Requests Settings

Twitch token is:

12 500 78

Twitch | Twitter @simontho... | Twitter Authy Twitter | Add Account

AT&T 10:16 AM

Google

Requests Settings

sthorpe@authy.com token is:

486 456

Google sthorpe@a... | Google sthorpe@t... | Google simonjame... | Google simon@trib...
Add Account

Lancaster University

Discussion: Your views on passwords

Computers and Cyber Security

Next Generation Programmers
9th June 2021
Dr Matthew Bradbury

The value of your information

Information is the new digital currency

- Information is **highly** valuable
- It is how many online companies (e.g., Google and Facebook) make money
- They build a profile about you, in order to target adverts to you

What are your:

- Interests / hobbies / activities
- Opinions

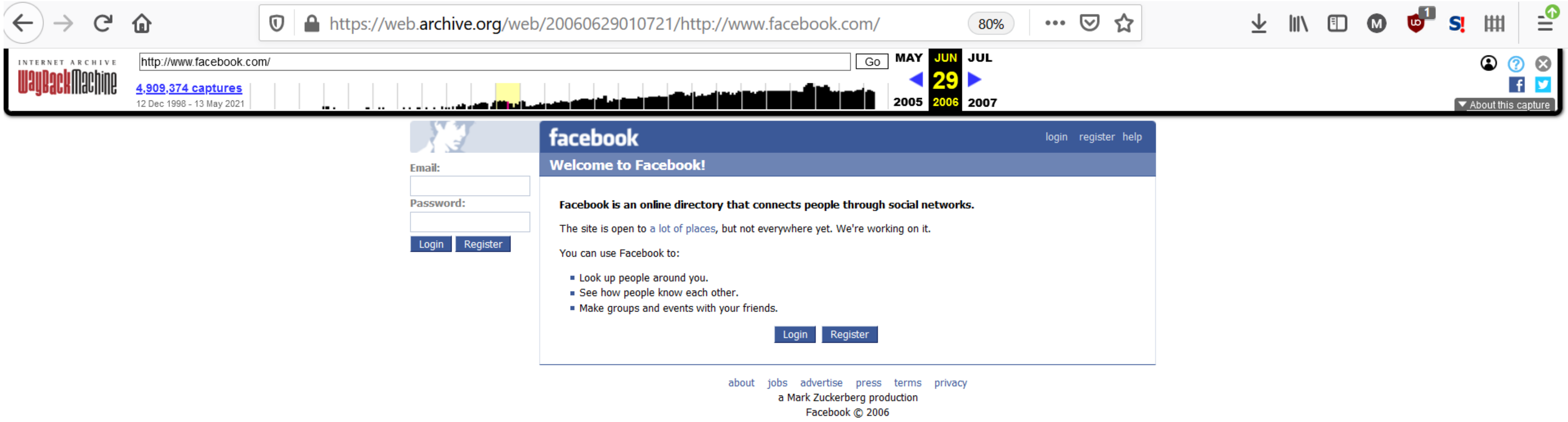
What is your:

- Age, Gender, Location, Income, Education Level, Personality

Who has a social media account?

Information on the internet is hard to remove

- Information posted publicly is hard to remove
- Sites like the Wayback Machine aim to archive the internet https://archive.org/web/



Welcome to Facebook!

Facebook is an online directory that connects people through social networks.

The site is open to a lot of places, but not everywhere yet. We're working on it.

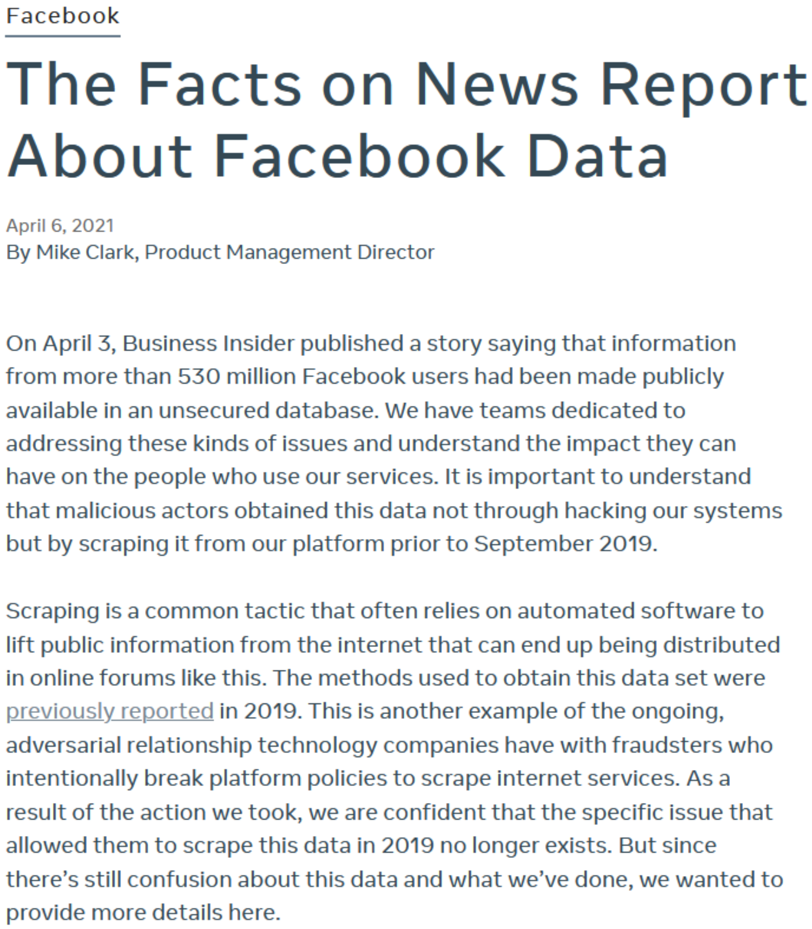
You can use Facebook to:

- Look up people around you.
- See how people know each other.
- Make groups and events with your friends.

a Mark Zuckerberg production
Facebook © 2006

Information on the internet is hard to remove

- People will write computer programs to **scrape** websites for information
- In April 2021 information on over 530 million Facebook accounts were scraped
- https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/



Facebook

The Facts on News Report About Facebook Data

April 6, 2021
By Mike Clark, Product Management Director

On April 3, Business Insider published a story saying that information from more than 530 million Facebook users had been made publicly available in an unsecured database. We have teams dedicated to addressing these kinds of issues and understand the impact they can have on the people who use our services. It is important to understand that malicious actors obtained this data not through hacking our systems but by scraping it from our platform prior to September 2019.

Scraping is a common tactic that often relies on automated software to lift public information from the internet that can end up being distributed in online forums like this. The methods used to obtain this data set were previously reported in 2019. This is another example of the ongoing, adversarial relationship technology companies have with fraudsters who intentionally break platform policies to scrape internet services. As a result of the action we took, we are confident that the specific issue that allowed them to scrape this data in 2019 no longer exists. But since there's still confusion about this data and what we've done, we wanted to provide more details here.

Lancaster University

What types of information do you share online?

Checking to see if you information has been leaked

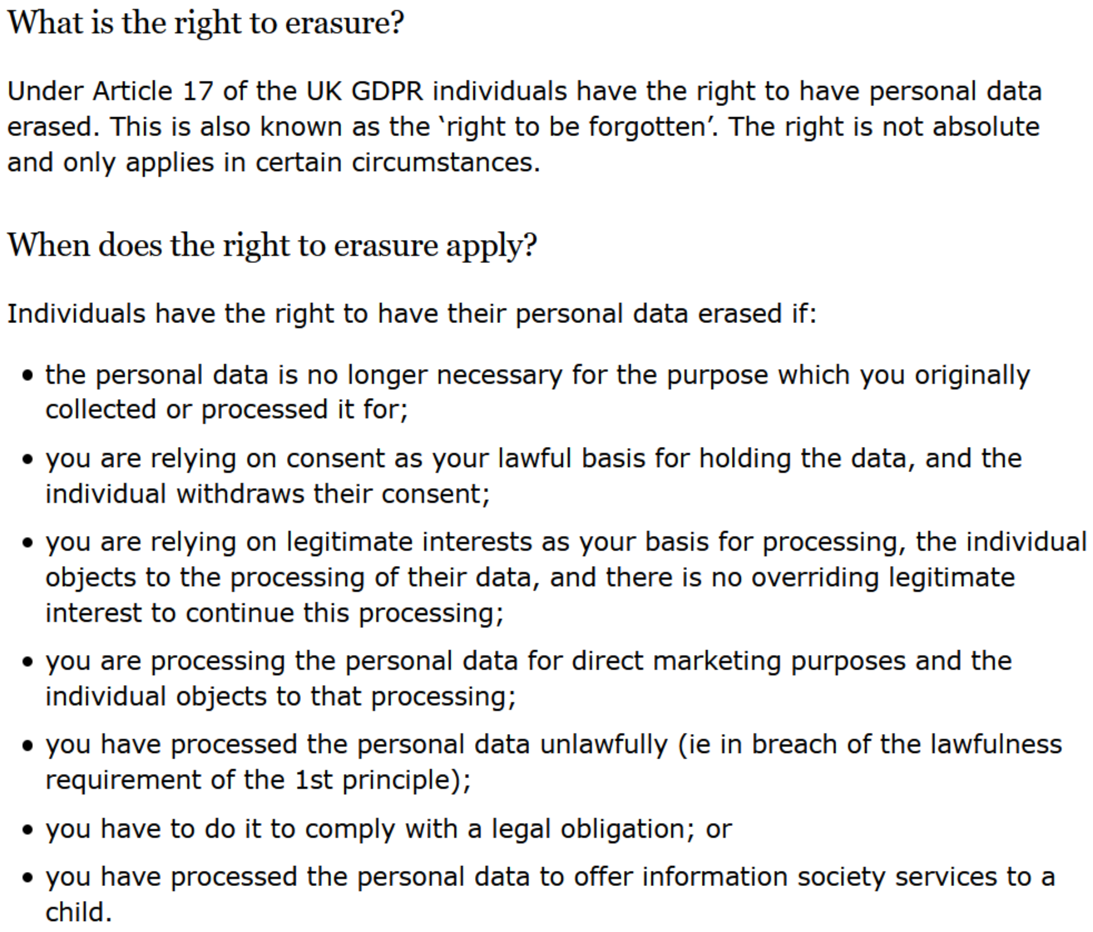
';--have i been pwned?

Check if your email or phone is in a data breach

- https://haveibeenpwned.com/
- Be careful that you use trustworthy sites! These websites can easily be used to steal your information too!

Laws exist in some places to be forgotten

- Some countries have laws on the “right to be forgotten”
- But only applies in some circumstances
- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/



What is the right to erasure?

Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

Rules when sharing online

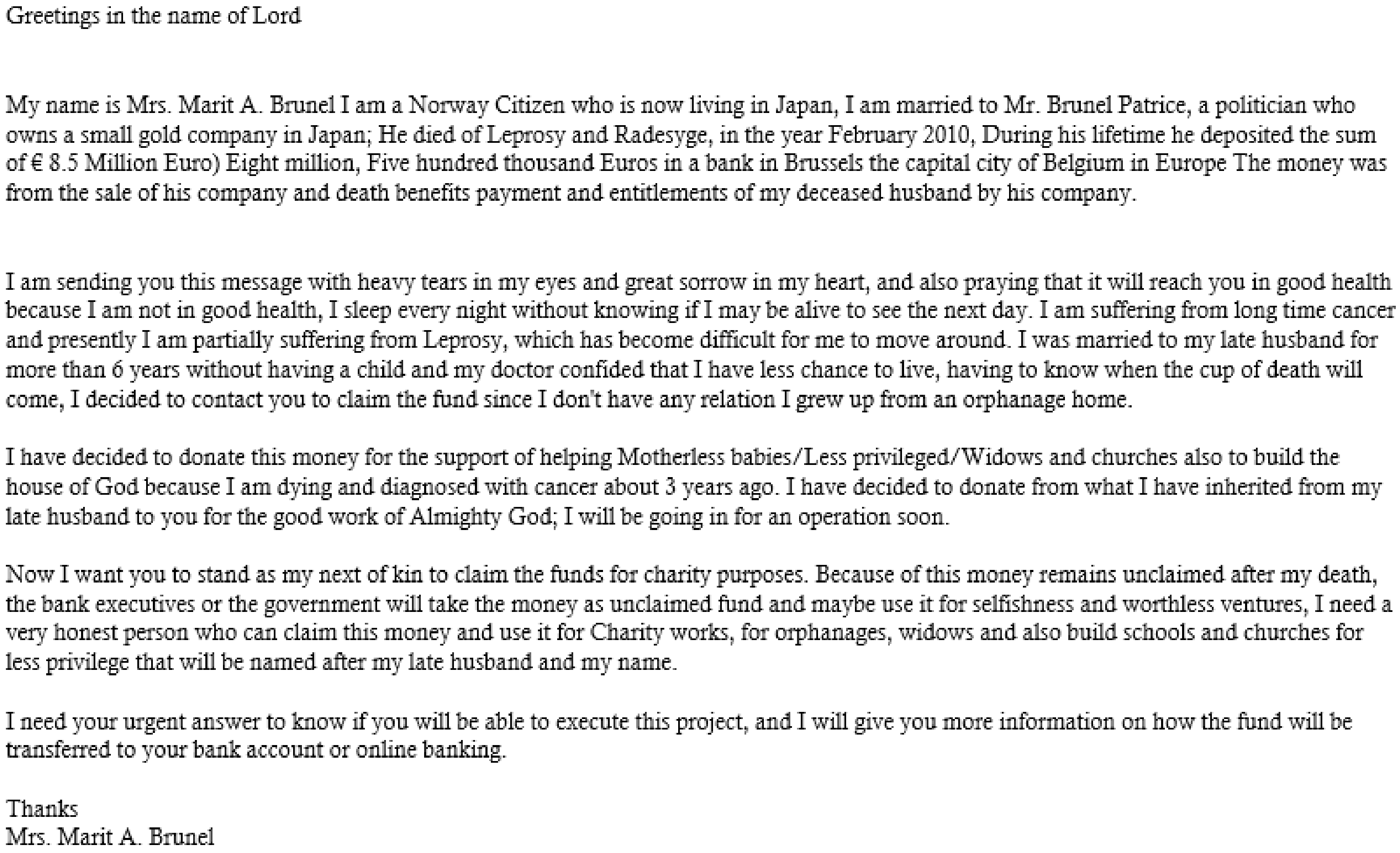
- Do not publicly share personal information (date of birth, location, phone number)
- Do not share any content (pictures/text) that you do not wish to be shared further
- Make sure to follow the rules of the website you are using

Lancaster University

Discussion: Your views on social media and information value

Recognising spam and email manipulation

Spam or not spam?



Greetings in the name of Lord

My name is Mrs. Marit A. Brunel I am a Norway Citizen who is now living in Japan, I am married to Mr. Brunel Patrice, a politician who owns a small gold company in Japan; He died of Leprosy and Radesyge, in the year February 2010, During his lifetime he deposited the sum of € 8.5 Million Euro) Eight million, Five hundred thousand Euros in a bank in Brussels the capital city of Belgium in Europe The money was from the sale of his company and death benefits payment and entitlements of my deceased husband by his company.

I am sending you this message with heavy tears in my eyes and great sorrow in my heart, and also praying that it will reach you in good health because I am not in good health, I sleep every night without knowing if I may be alive to see the next day. I am suffering from long time cancer and presently I am partially suffering from Leprosy, which has become difficult for me to move around. I was married to my late husband for more than 6 years without having a child and my doctor confided that I have less chance to live, having to know when the cup of death will come, I decided to contact you to claim the fund since I don't have any relation I grew up from an orphanage home.

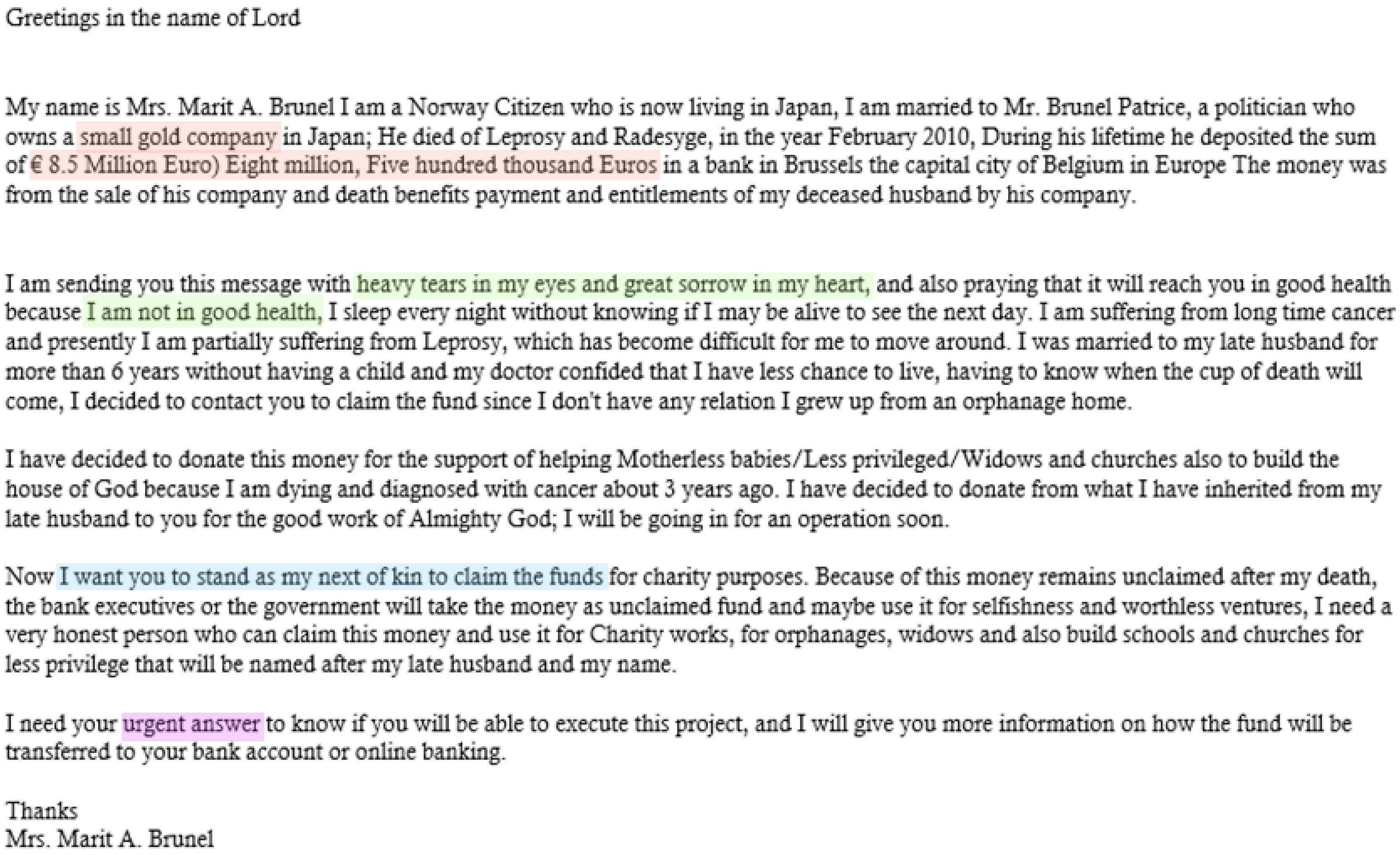
I have decided to donate this money for the support of helping Motherless babies/Less privileged/Widows and churches also to build the house of God because I am dying and diagnosed with cancer about 3 years ago. I have decided to donate from what I have inherited from my late husband to you for the good work of Almighty God; I will be going in for an operation soon.

Now I want you to stand as my next of kin to claim the funds for charity purposes. Because of this money remains unclaimed after my death, the bank executives or the government will take the money as unclaimed fund and maybe use it for selfishness and worthless ventures, I need a very honest person who can claim this money and use it for Charity works, for orphanages, widows and also build schools and churches for less privilege that will be named after my late husband and my name.

I need your urgent answer to know if you will be able to execute this project, and I will give you more information on how the fund will be transferred to your bank account or online banking.

Thanks
Mrs. Marit A. Brunel

Spam!



Greetings in the name of Lord

My name is Mrs. Marit A. Brunel I am a Norway Citizen who is now living in Japan, I am married to Mr. Brunel Patrice, a politician who owns a small gold company in Japan; He died of Leprosy and Radesyge, in the year February 2010, During his lifetime he deposited the sum of € 8.5 Million Euro) Eight million, Five hundred thousand Euros in a bank in Brussels the capital city of Belgium in Europe The money was from the sale of his company and death benefits payment and entitlements of my deceased husband by his company.

I am sending you this message with heavy tears in my eyes and great sorrow in my heart, and also praying that it will reach you in good health because I am not in good health, I sleep every night without knowing if I may be alive to see the next day. I am suffering from long time cancer and presently I am partially suffering from Leprosy, which has become difficult for me to move around. I was married to my late husband for more than 6 years without having a child and my doctor confided that I have less chance to live, having to know when the cup of death will come, I decided to contact you to claim the fund since I don't have any relation I grew up from an orphanage home.

I have decided to donate this money for the support of helping Motherless babies/Less privileged/Widows and churches also to build the house of God because I am dying and diagnosed with cancer about 3 years ago. I have decided to donate from what I have inherited from my late husband to you for the good work of Almighty God; I will be going in for an operation soon.

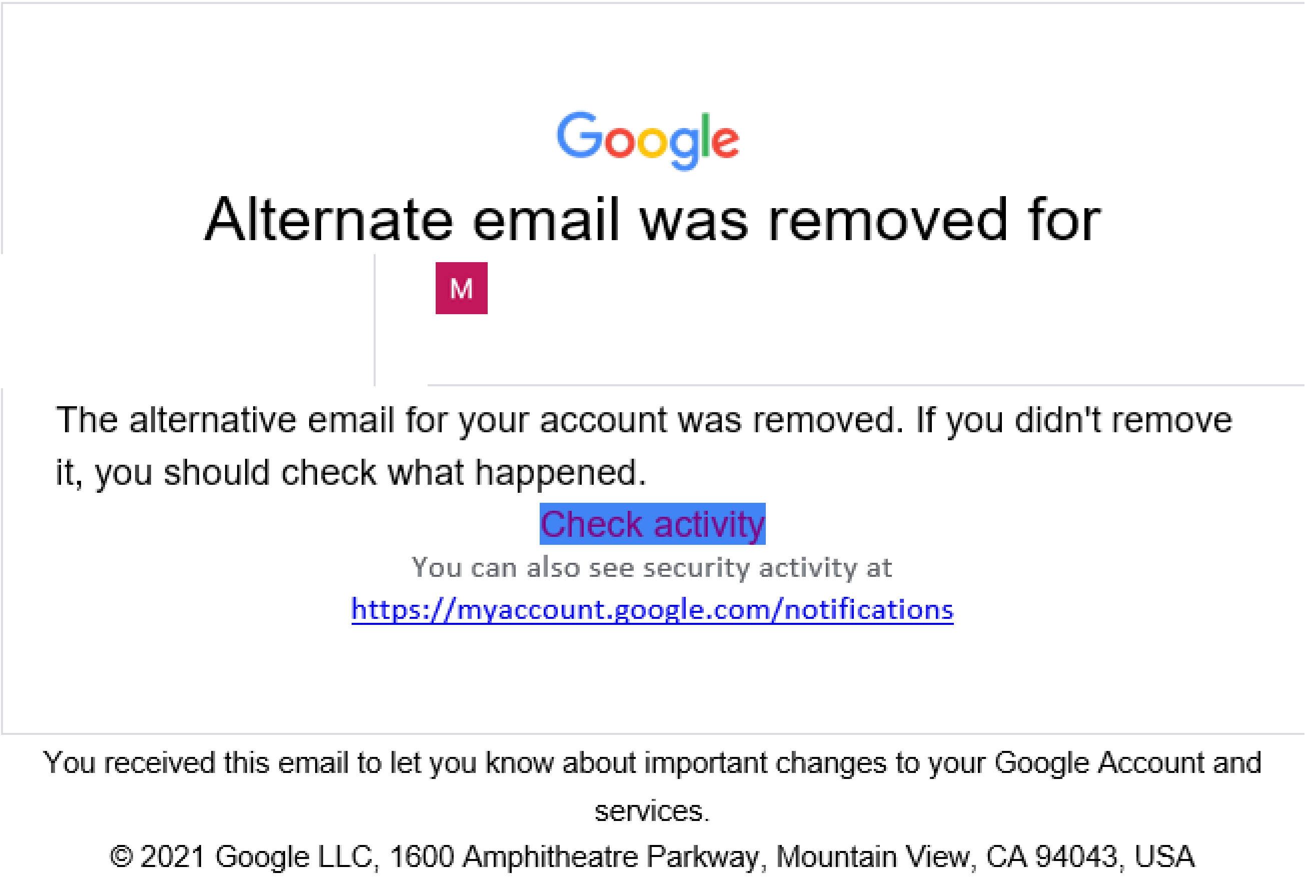
Now I want you to stand as my next of kin to claim the funds for charity purposes. Because of this money remains unclaimed after my death, the bank executives or the government will take the money as unclaimed fund and maybe use it for selfishness and worthless ventures, I need a very honest person who can claim this money and use it for Charity works, for orphanages, widows and also build schools and churches for less privilege that will be named after my late husband and my name.

I need your urgent answer to know if you will be able to execute this project, and I will give you more information on how the fund will be transferred to your bank account or online banking.

Thanks
Mrs. Marit A. Brunel

1. A large amount of money
2. They are not in good health
3. They want you to claim the money
4. It needs to be done urgently

Spam or not spam?



Alternate email was removed for

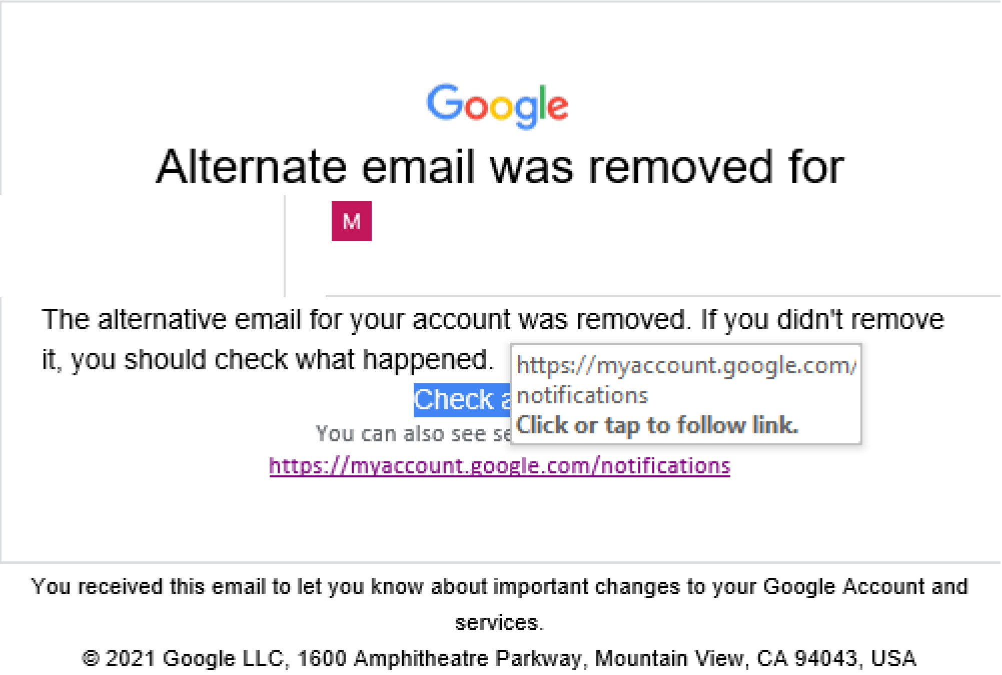
The alternative email for your account was removed. If you didn't remove it, you should check what happened.

You can also see security activity at
https://myaccount.google.com/notifications

You received this email to let you know about important changes to your Google Account and services.

© 2021 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Not spam!



Google

Alternate email was removed for

M

The alternative email for your account was removed. If you didn't remove it, you should check what happened.

Check a

https://myaccount.google.com/
notifications
Click or tap to follow link.

You can also see se

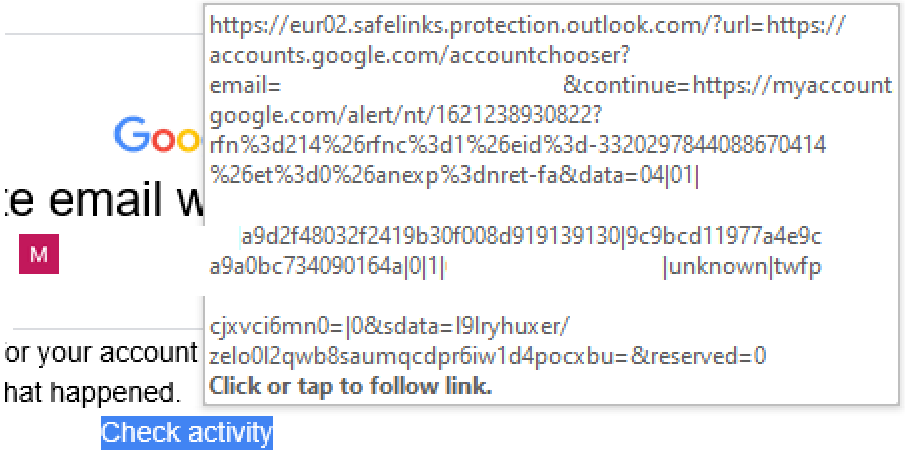
https://myaccount.google.com/notifications

You received this email to let you know about important changes to your Google Account and services.

© 2021 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

1. Check links for validity before clicking on them
2. Was this an email that you expected?

Visit the website directly instead of clicking on any of the links in the email



Goo

:e email w

M

or your account

hat happened.

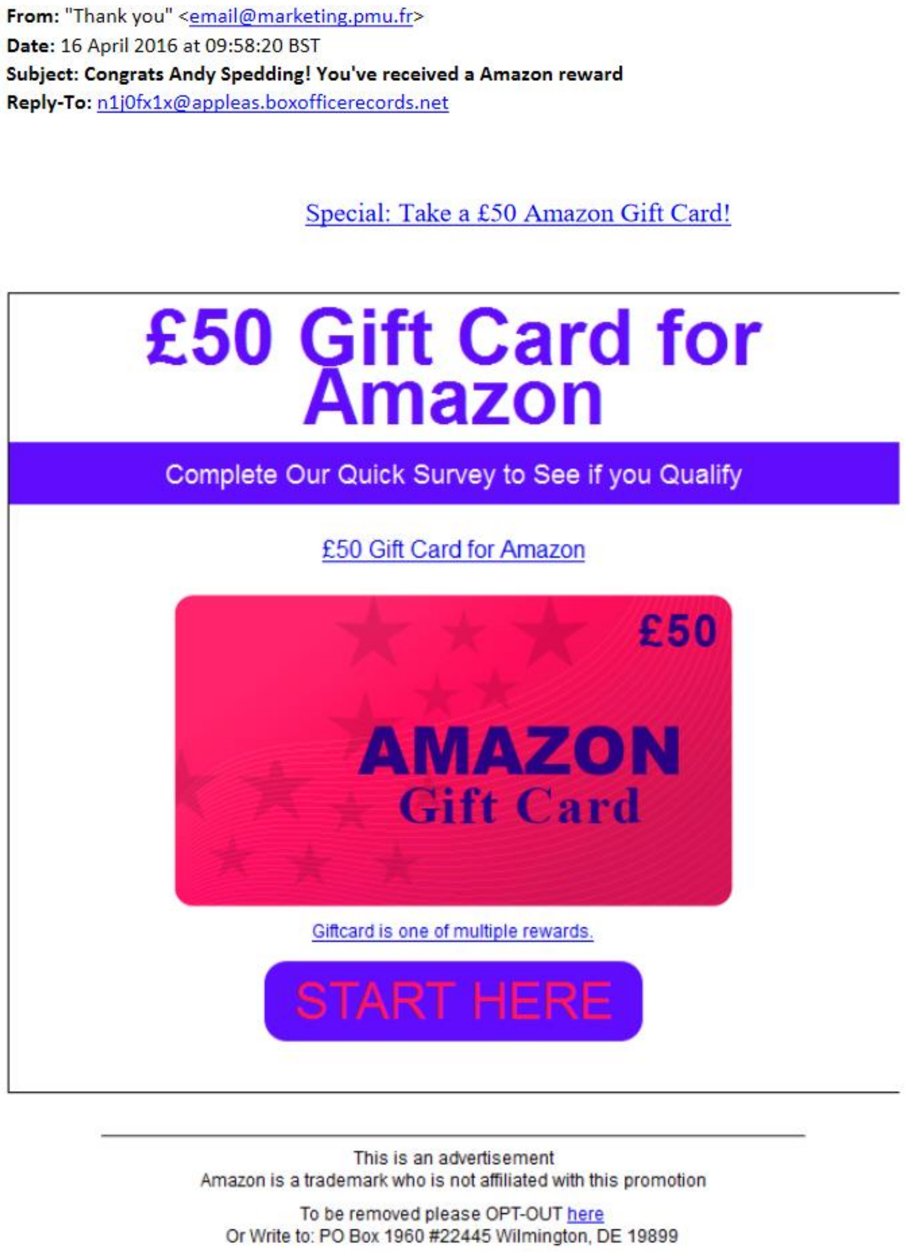
Check activity

https://eur02.safelinks.protection.outlook.com/?url=https://
accounts.google.com/accountchooser?
email= &continue=https://myaccount
google.com/alert/nt/1621238930822?
rfn%3d214%26rfnc%3d1%26eid%3d-3320297844088670414
%26et%3d0%26anexp%3dnret-fa&data=04|01|

a9d2f48032f2419b30f008d919139130|9c9bcd11977a4e9c
a9a0bc734090164a|0|1| |unknown|twfp

cjxvci6mn0=|0&sdata=l9lryhuxer/
zelo0l2qwb8saumqcdpr6iw1d4pocxbu=&reserved=0
Click or tap to follow link.

Spam or not Spam?



From: "Thank you" <email@marketing.pmu.fr>
Date: 16 April 2016 at 09:58:20 BST
Subject: Congrats Andy Spedding! You've received a Amazon reward
Reply-To: n1j0fx1x@appleas.boxofficerecords.net

Special: Take a £50 Amazon Gift Card!

£50 Gift Card for Amazon

Complete Our Quick Survey to See if you Qualify

£50 Gift Card for Amazon

Giftcard is one of multiple rewards.

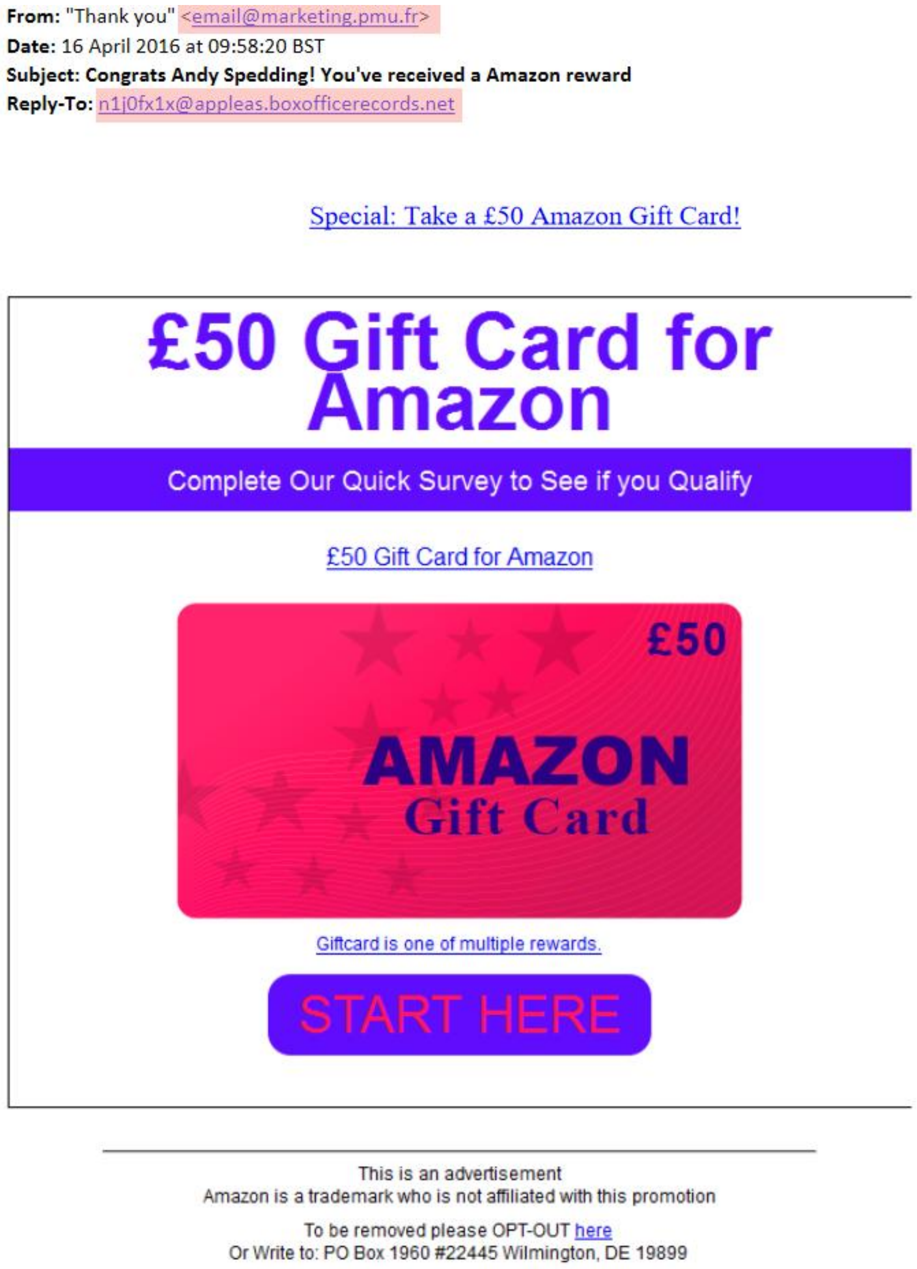
START HERE

This is an advertisement
Amazon is a trademark who is not affiliated with this promotion

To be removed please OPT-OUT here
Or Write to: PO Box 1960 #22445 Wilmington, DE 19899

Spam!

- From and Reply-To differ
- The link is to a shortened URL, to hard to know what the target actual is http://bit.ly/...
- Why are they giving you free money?



From: "Thank you" <email@marketing.pmu.fr>
Date: 16 April 2016 at 09:58:20 BST
Subject: Congrats Andy Spedding! You've received a Amazon reward
Reply-To: n1j0fx1x@appleas.boxofficerecords.net

Special: Take a £50 Amazon Gift Card!

£50 Gift Card for Amazon

Complete Our Quick Survey to See if you Qualify

£50 Gift Card for Amazon

Giftcard is one of multiple rewards.

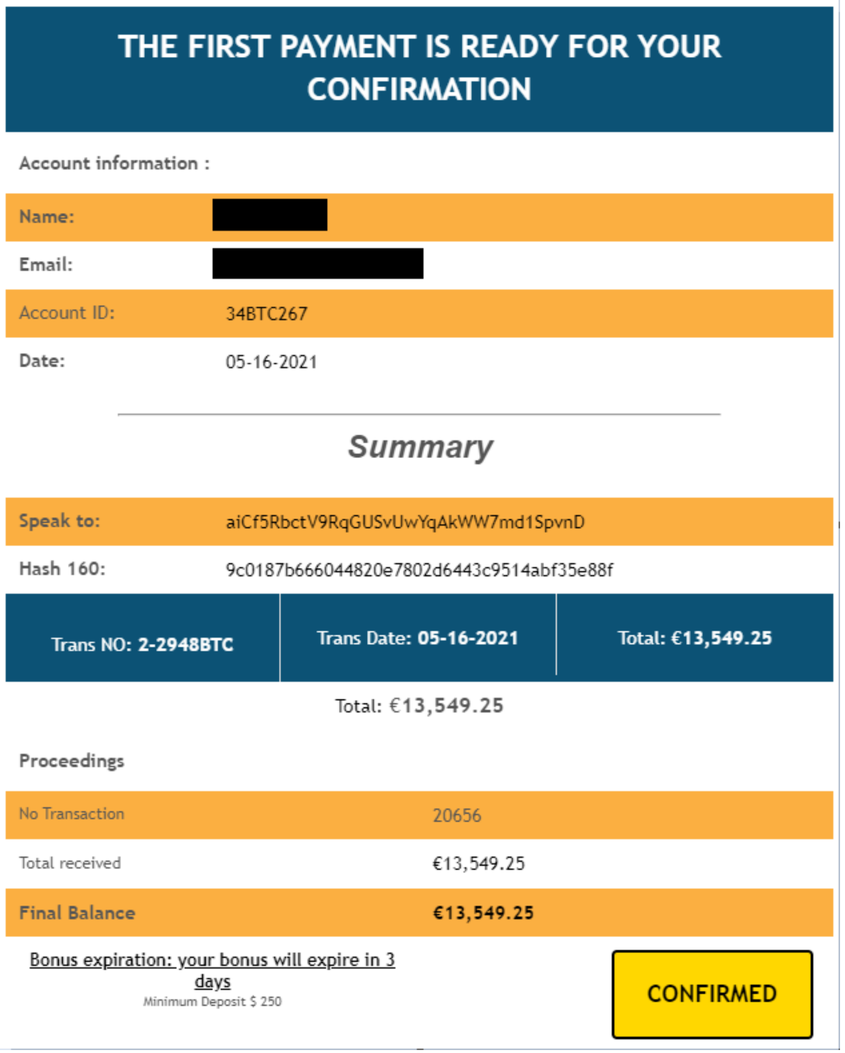
START HERE

This is an advertisement
Amazon is a trademark who is not affiliated with this promotion

To be removed please OPT-OUT here
Or Write to: PO Box 1960 #22445 Wilmington, DE 19899

Source: https://as.exeter.ac.uk/media/level1/academicserviceswebsite/it/documents/Examples_of_spam_and_phishing_emails.pdf

Spam or not Spam?



THE FIRST PAYMENT IS READY FOR YOUR CONFIRMATION

Account information :

Name:	[redacted]
Email:	[redacted]
Account ID:	34BTC267
Date:	05-16-2021

Summary

Speak to:	aiCf5RbctV9RqGUSvUwYqAkWW7md1SpvnD
Hash 160:	9c0187b666044820e7802d6443c9514abf35e88f

Trans NO: **2-2948BTC**	Trans Date: **05-16-2021**	Total: **€13,549.25**

Total: €13,549.25

Proceedings

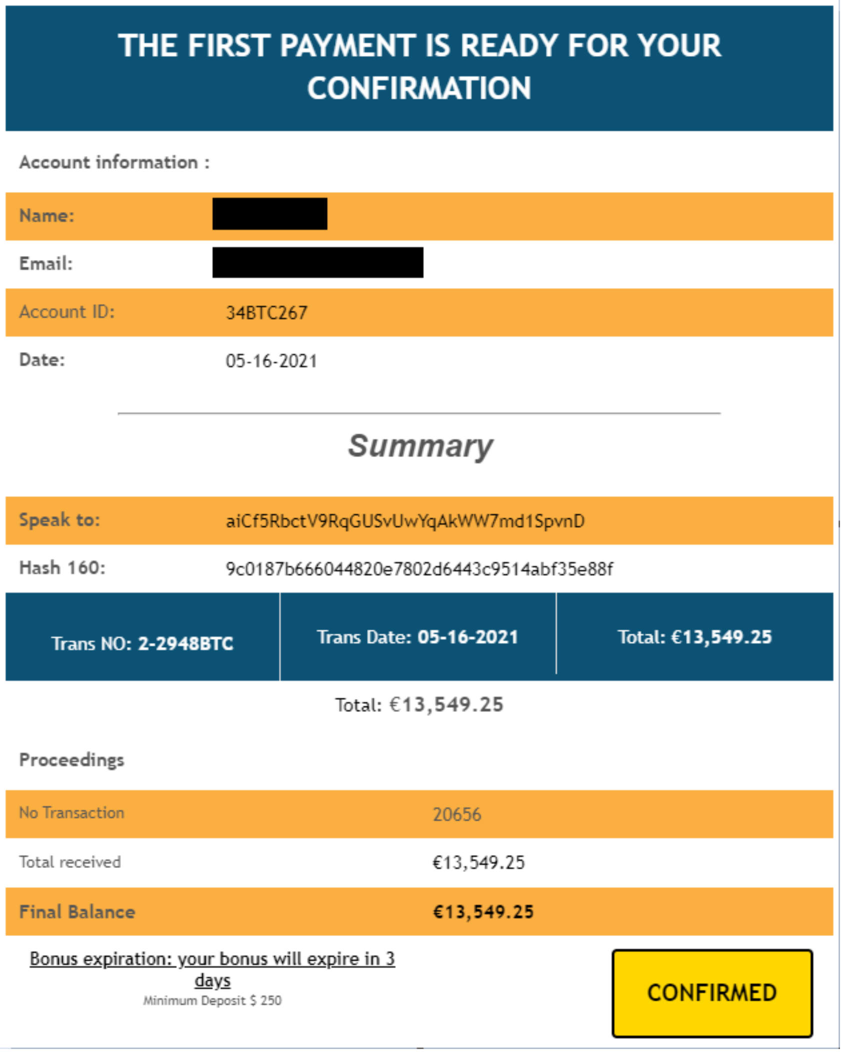
No Transaction	20656
Total received	€13,549.25
Final Balance	**€13,549.25**

Bonus expiration: your bonus will expire in 3 days

Minimum Deposit $ 250

Spam!

- Why are they giving you free money?
- You need to pay $250 first



THE FIRST PAYMENT IS READY FOR YOUR CONFIRMATION

Account information :

Name:	[redacted]
Email:	[redacted]
Account ID:	34BTC267
Date:	05-16-2021

Summary

Speak to:	aiCf5RbctV9RqGUSvUwYqAkWW7md1SpvnD
Hash 160:	9c0187b666044820e7802d6443c9514abf35e88f

Trans NO: **2-2948BTC**	Trans Date: **05-16-2021**	Total: **€13,549.25**

Total: €13,549.25

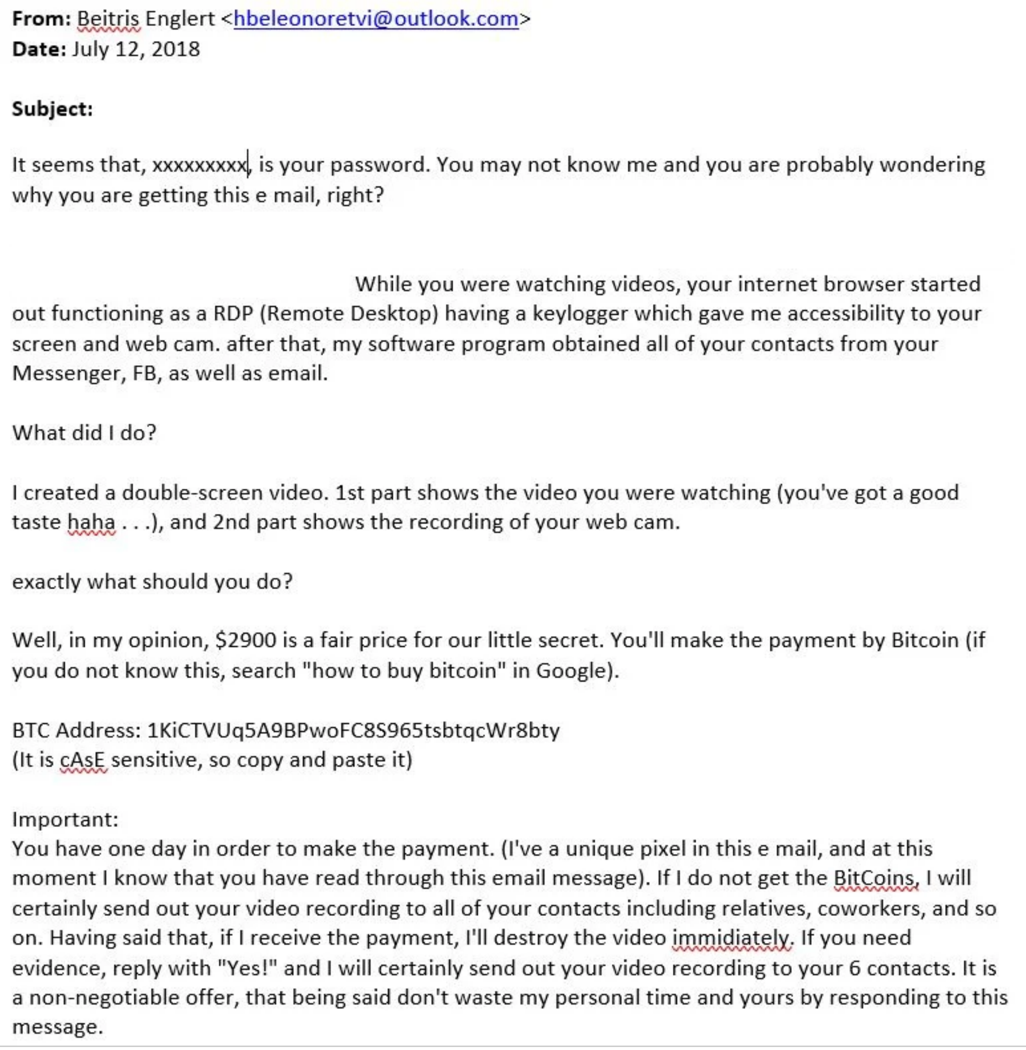
Proceedings

No Transaction	20656
Total received	€13,549.25
Final Balance	**€13,549.25**

Bonus expiration: your bonus will expire in 3 days

Minimum Deposit $ 250

Spam or not Spam?



From: Beitris Englert <hbeleonoretvi@outlook.com>
Date: July 12, 2018

Subject:

It seems that, xxxxxxxxx, is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

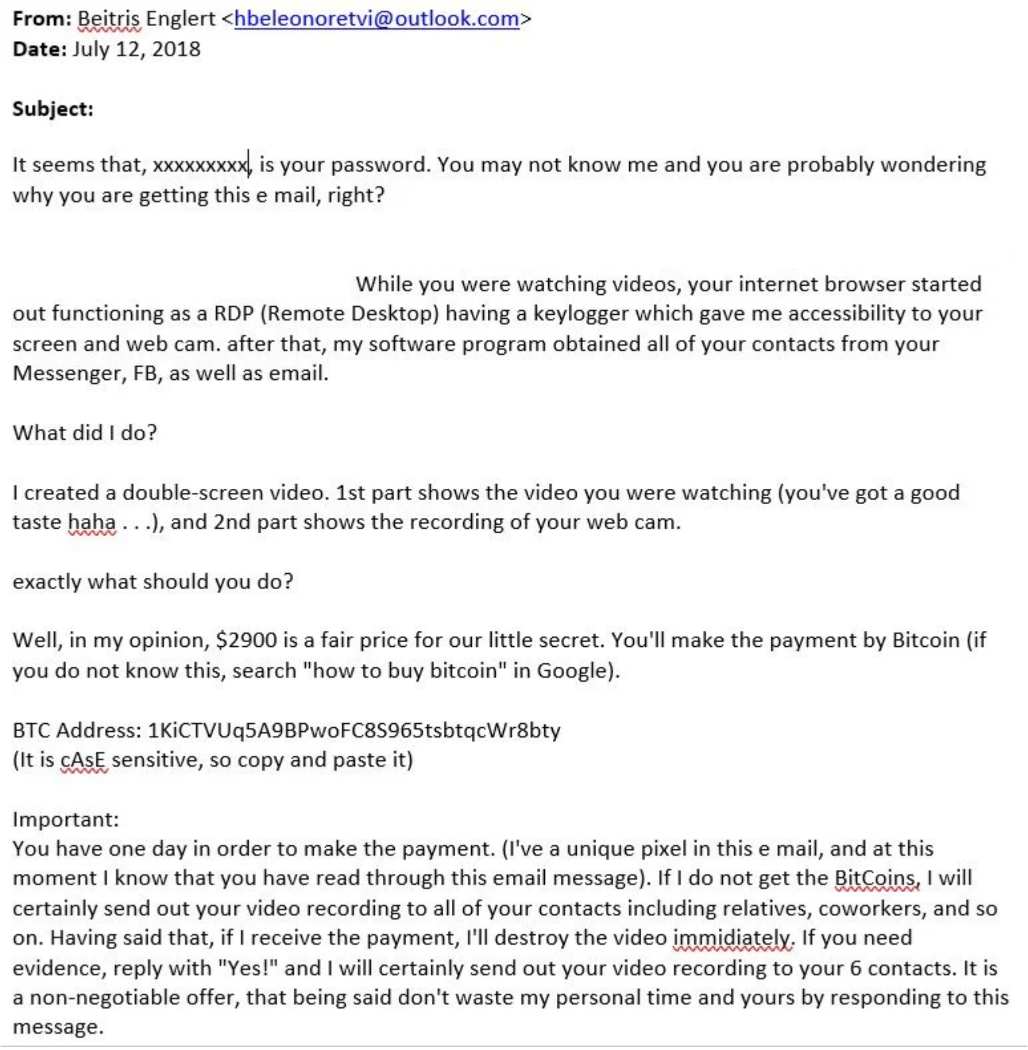
Well, in my opinion, $2900 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
(It is cAsE sensitive, so copy and paste it)

Important:
You have one day in order to make the payment. (I've a unique pixel in this e mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

Extortion!

- A password is leaked from a website
- Scammers try to use this information to extort money out of their target
- This is illegal in many countries (including Kazakhstan)



From: Beitris Englert <hbeleonoretvi@outlook.com>
Date: July 12, 2018

Subject:

It seems that, xxxxxxxxx, is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $2900 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
(It is cAsE sensitive, so copy and paste it)

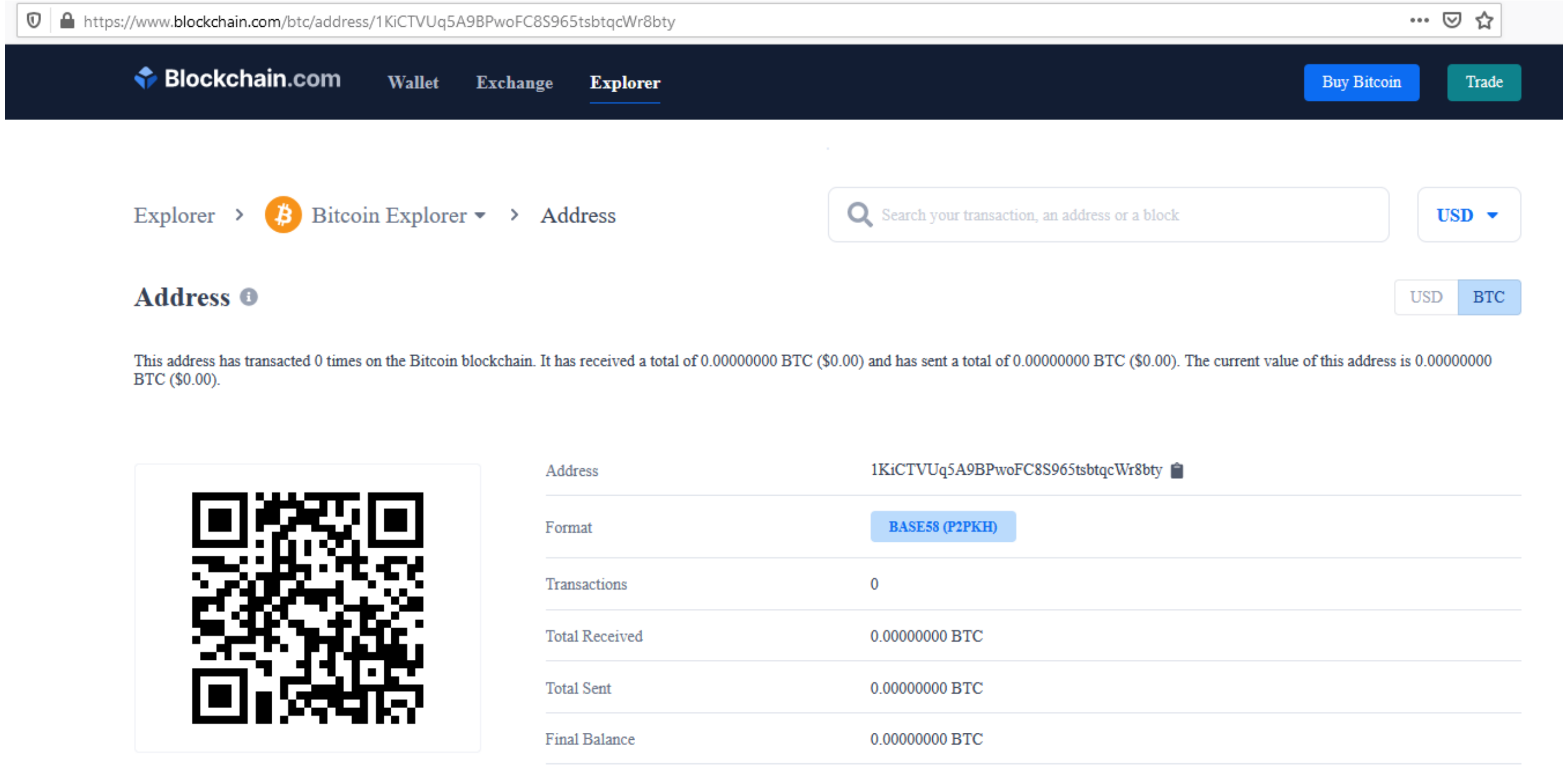
Important:
You have one day in order to make the payment. (I've a unique pixel in this e mail, and at this moment I know that you have read through this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, I'll destroy the video immidiately. If you need evidence, reply with "Yes!" and I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message.

Source: https://www.bleepingcomputer.com/news/security/beware-of-extortion-scams-stating-they-have-video-of-you-on-adult-sites/

Article 194 https://adilet.zan.kz/eng/docs/K1400000226

Did it work?

- No!
- We can check the bitcoin wallet to see what transactions have been made
- Other scams have unfortunately worked



https://www.blockchain.com/btc/address/1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty

Blockchain.com
Wallet
Exchange
Explorer
Buy Bitcoin
Trade
Explorer › Bitcoin Explorer › Address
Search your transaction, an address or a block
USD
USD
BTC

Address

This address has transacted 0 times on the Bitcoin blockchain. It has received a total of 0.00000000 BTC ($0.00) and has sent a total of 0.00000000 BTC ($0.00). The current value of this address is 0.00000000 BTC ($0.00).

Address	1KiCTVUq5A9BPwoFC8S965tsbtqcWr8bty
Format	BASE58 (P2PKH)
Transactions	0
Total Received	0.00000000 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00000000 BTC

Techniques to check email validity

- Do not rely on the email having been addressed to you by name
- If in doubt, do not click links on the email, go to the website directly

- If the email is too good to be true, it probably is
- If you are being offered money, try to think what the sender has to gain

Discussion: Your views on spam and email manipulation

Lancaster University

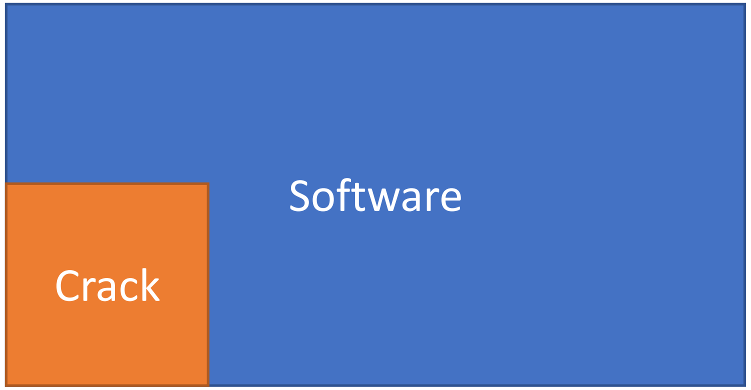
Computers and Cyber Security

Next Generation Programmers
11th June 2021
Dr Matthew Bradbury

Alternatives to pirated software

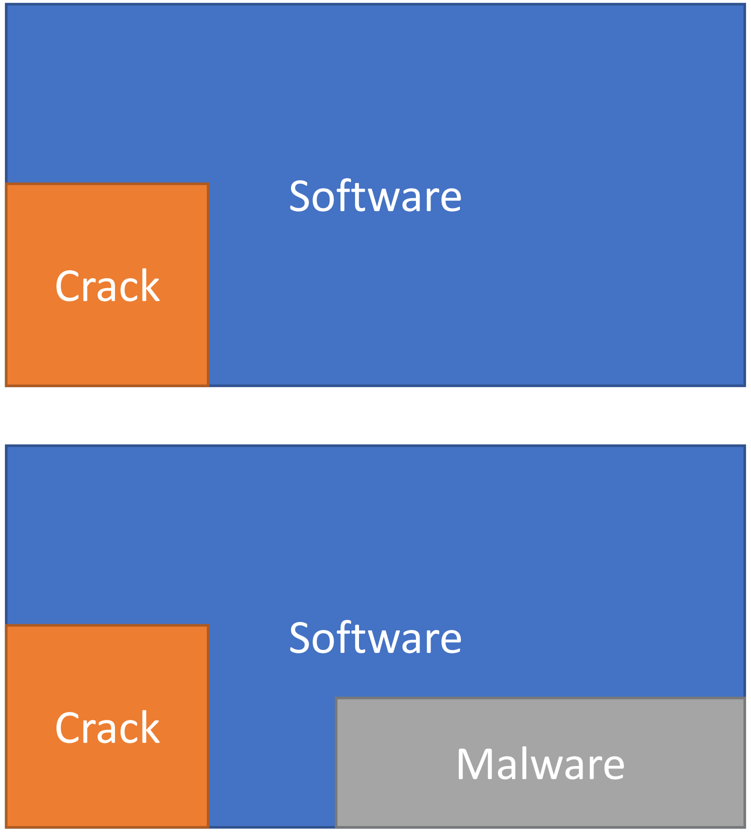
Pirating Software

- Software can be very expensive
- It may seem easy to download and use a “cracked” version instead
- Pirates can edit software to remove licence checks
- However, there are a number of risks



Risks to Pirating Software

- Software can also be edited to include malicious code
- Pirated software is unlikely to be updated, so may contain vulnerabilities



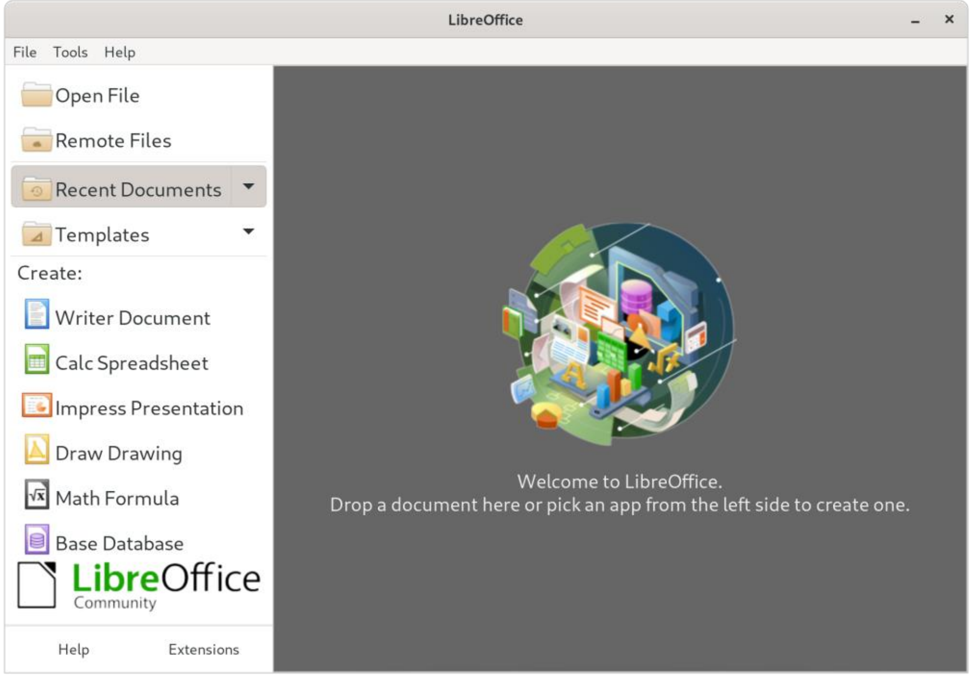
What kinds of malware might be included?

- **Keyloggers and Spyware** – To steal your passwords and information
- **Ransomware** – Which encrypts your files and demands payment
- **Cryptocurrency Miners** – Which steal your computers processing power to mine cryptocurrency
- **Adware** – That show intrusive and unwanted adverts on your computer
- **Botnets** – That use your computer to attack others on the internet
- **Trojans** – That allow attackers access to your computer

Alternatives to Pirating Software

- Lots of software can be used for free!
- You can create and edit documents using LibreOffice
- https://www.libreoffice.org/

LibreOffice
The Document Foundation



Welcome to LibreOffice.
Drop a document here or pick an app from the left side to create one.

Alternatives to Pirating Software

- You don’t even need to use Windows or MacOS
- Free Operating Systems are available
  - You will need to use different programs
  - You will need to learn how to use a different operating system
- Ubuntu is one example, but there are many others

ubuntu

Why does this software exist?

- There is a philosophy to provide “free” software (also described as “libre”)
- What does free mean?

Free Beer
(you do not need to pay money)

Freedom
Freedom to use, modify and share software

What freedoms do you get?

1. Run the program as you wish
2. Study the program and change it (look at the code)
3. Redistribute copies
4. Redistribute copies of modified versions

The aim is for you to be able to benefit the entire community with your work!

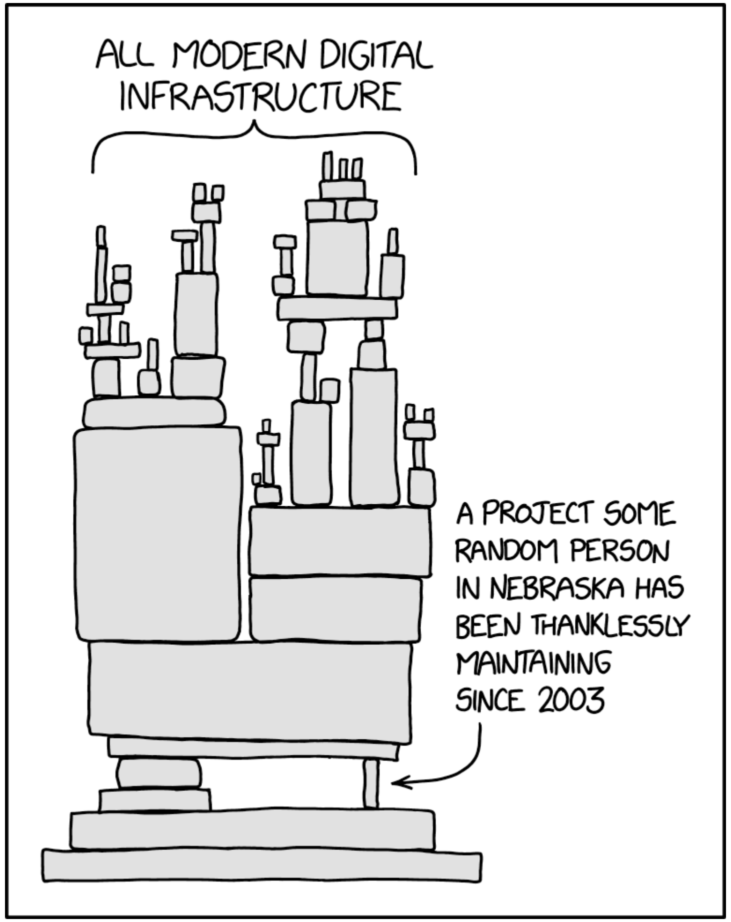
(https://www.gnu.org/philosophy/free-sw.html)

What are the advantages?

- The community works together to improve software
- Allows the source code of programs to be inspected
- This includes identifying and fixing security vulnerabilities

What are the risks?

- It takes time to maintain this software
- Many people do this work as a hobby
- Some foundations pay people to work on this software
- There is a risk that critical dependencies are not adequately maintained


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Randall Munroe https://xkcd.com/2347/

Risks – Case Study

- OpenSSL
- A core aspect of secure internet communications
- Multiple vulnerabilities found in it due to lack of resources (mid 2010s)
- Identified as critical, so has since received further investment

https://heartbleed.com

Lancaster University

Discussion: Your views on free software

Lancaster University

Software and Cybersecurity Skills

The need for these skills

- There is a lack of people around the world with good software development skills
- There are also lots of malicious (bad) actors and a lack of people with the skills to defend systems from them
- Access to the internet means that anyone from around the world can interact with others with ease
- For projects where the source code is public, you can contribute and fix issues that you encounter

The importance to use skills ethically

- With computer skills there is the importance that they are not used to cause harm to others
- It can be easy to do, even unintentionally

1. Do not prevent the correct operation of a computing system
2. Do not steal from others (including data and money)
3. If you encounter an issue, ensure that you responsibly disclose it

Remember – there are real people behind the screen

What have we learnt?

- How to make a strong password
- The value of your information
- How to recognise spam and email manipulation
- Alternatives to pirating software
- The worldwide usefulness of computer and cyber security skills

Lancaster University

Thank you for attending!