Danske Bank

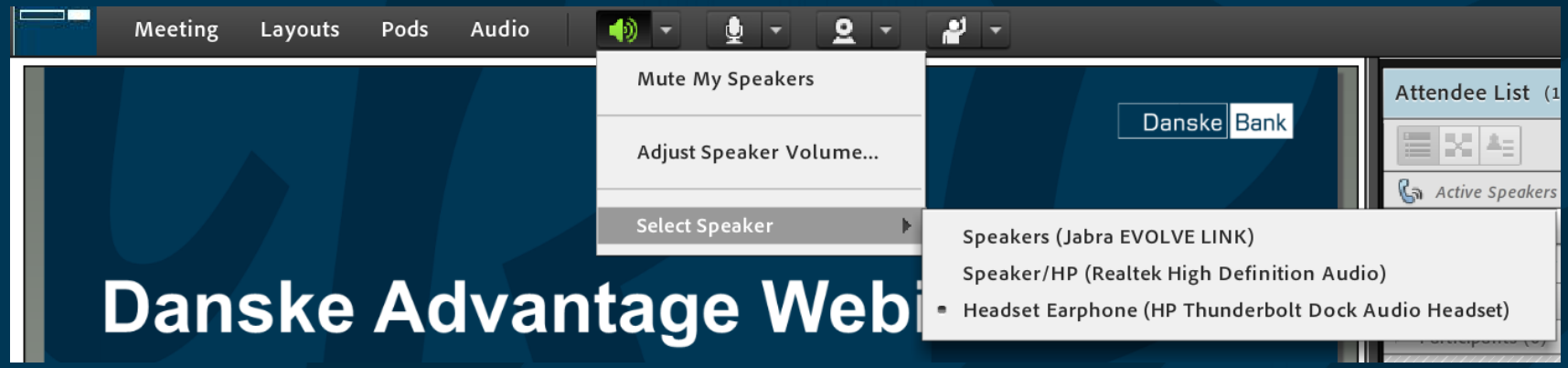
Danske Advantage Webinar Series

Fraud, Scams and Cyber Security

Wednesday 19 August 2020
11am - 12pm

Housekeeping

Please check you have enabled your headset/ speaker by clicking on the dropdown arrow next to the Speaker Icon at the top of your screen. Then select the correct speaker option. If you still can't hear, go to Settings/ System/ Sound and select your headset/integrated speaker



Your mic's will be muted during the presentations but you can ask questions as we go along by typing them into the Q&A chatbox.

Please bear with us if our Wifi connectivity drops or the technology falters, we will be back up and running as soon as we can.

Danske Bank

Cyber Security

Philip has over 20 years' industrial experience in software development in financial and capital markets and the telecoms sectors. Philip is the Course Director for the MSc in Applied Security and lecturer researching malware and secure software development at CSIT (Centre for Secure Information Technologies) at Queen's University .

Dr Philip O'Kane
Lecturer, Network Security Systems, Queens University Belfast

Danske Bank

Fraud, Scams and Cyber Security

Dr. Philip O'Kane

August 2020

Queen's University Belfast & CSIT

Cyber Security at QUB

The Centre for Secure Information Technologies (CSIT) is the UK's national Innovation and Knowledge Centre (IKC) for cyber security.

- 88 people (academics, researchers, experienced engineers and business development staff) focused on research impact and commercial exploitation.
- CSIT is also a GCHQ "Academic Centre of Excellence in Cyber Security Research"
- CSIT was honoured by the Queen for its work in "strengthening global cyber security"

QUEEN'S UNIVERSITY BELFAST

THE QUEEN'S ANNIVERSARY PRIZES
FOR HIGHER AND FURTHER EDUCATION
2015

Cyber Security programs - Applied MSc & Undergraduate

Programme Aims:

- Develop the next generation of industry leaders & address the shortage of cyber security professionals globally
- Provide graduates with a comprehensive understanding of the cyber security challenges facing industry & society
- Equip graduates with the skills necessary to address those challenges

GCHQ Certified Education
Master's Degree in Cyber Security

GCHQ/NCSC fully certified Master's Degree

QUEEN'S UNIVERSITY BELFAST

Webinar content

- Attack Surface
  - Software
  - Humans
- Types of attacks
  - Social Engineering
  - Credential loss (password)
- Prevent password disclosure/leakage
  - Password storage
  - Password hacking
  - Human behaviour
- Multi-Factor Authentication (MFA)

QUEEN'S UNIVERSITY BELFAST

Modern Banking

Convenience:

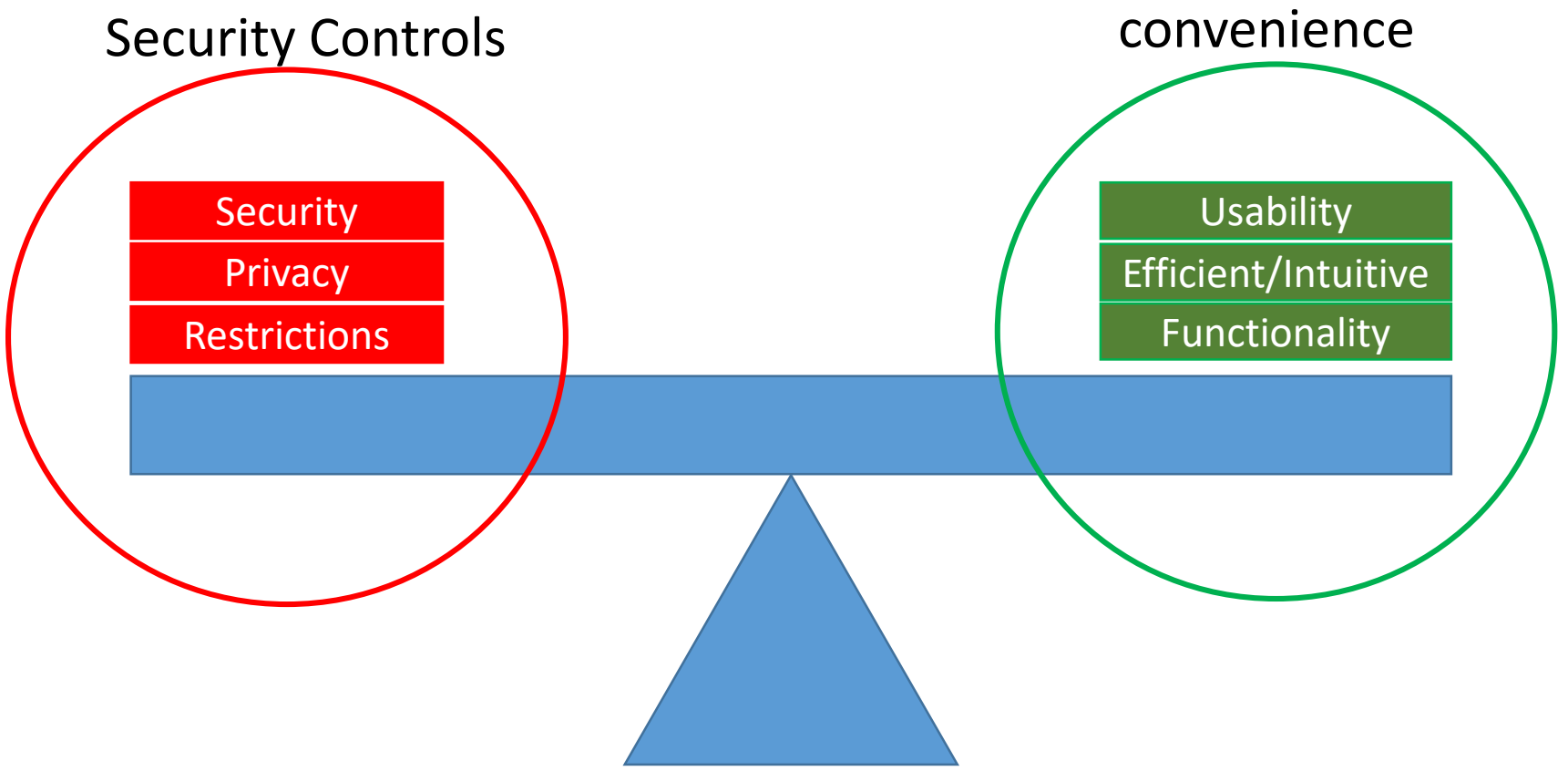
- **We can manage our own transactions with few visits to the Bank**
- **Faster transactions**
- **Monitor transactions**
- **Business can integrate into the accounting software**

Improvements:

- **Cost of doing business**
- **Cash in transits heist – DOWN,**
- **Pick-pockets and mugging get away with less**

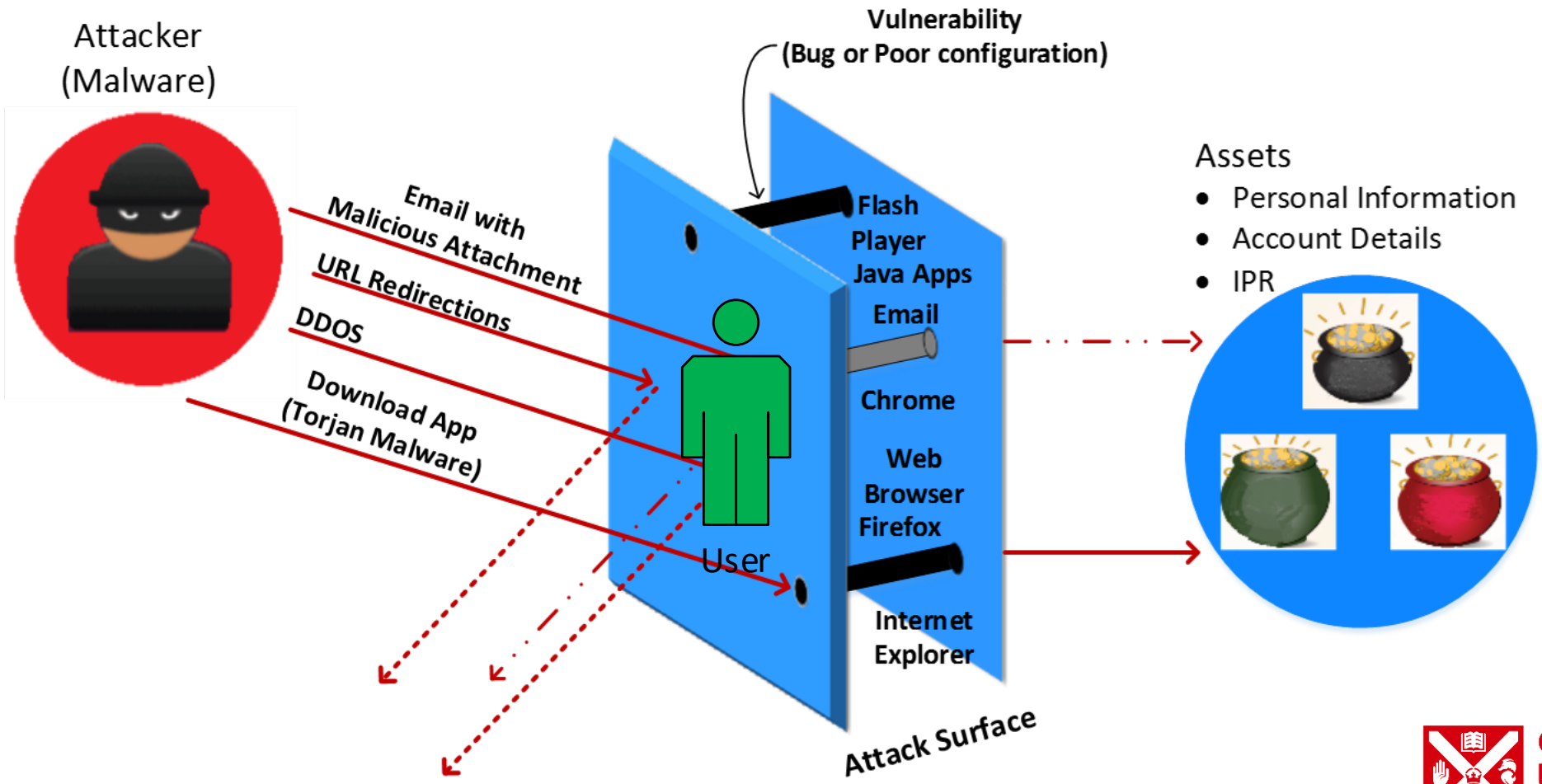
QUEEN'S UNIVERSITY BELFAST

Modern Banking



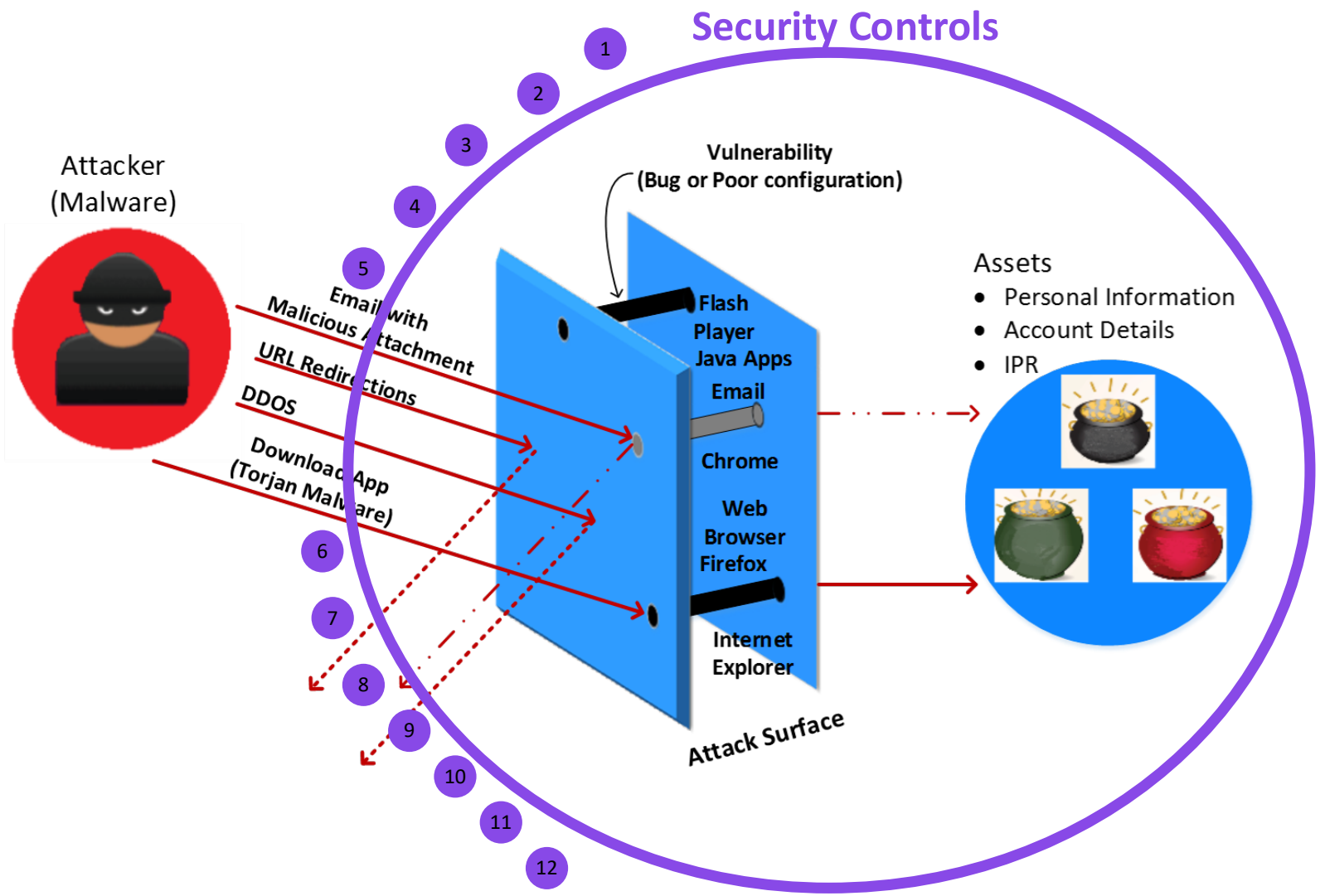
QUEEN'S UNIVERSITY BELFAST

What is the attack surface?



QUEEN'S UNIVERSITY BELFAST

How do we control the attack surface?



QUEEN'S UNIVERSITY BELFAST

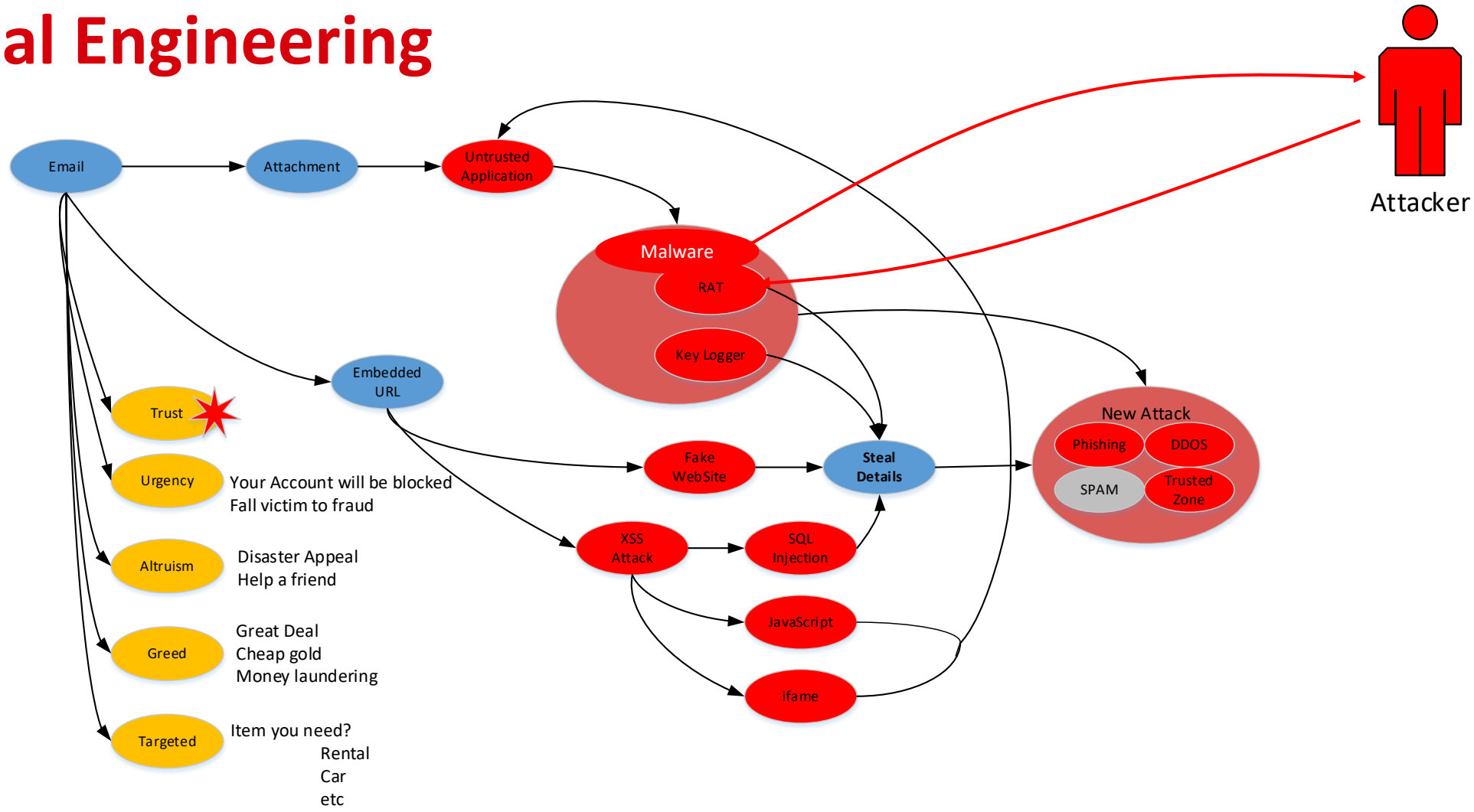
The Target

Most attacks target people

- Yes, technology is targeted, but as we improve the technology criminals target the weakness link
  - “People Problem”
- Increasingly sophisticated Social Engineering
  - Information harvesting, social media, direct contact – tailored attacks
  - Request verification of information and warn of some consequence if not provided
- Are we asking too much of users?
  - Complex password, multiple accounts
  - Detect social engineering attacks

QUEEN'S UNIVERSITY BELFAST

Social Engineering



QUEEN'S UNIVERSITY BELFAST

How does the attacker target you?

Malware = **mal**icious software

- Ransomware
- Bot, a robotic software application controlled by another
- Remote Access Tool, Backdoor (RAT)
- Spyware, Memory scrapper, Adware etc.

Malware symptoms

- Often NONE!!!
- Until:
  - Your files are locked
  - Your bank balance is empty
  - Pivot attack - work colleague is compromised, friends attacked, DDoS attack …
- Antivirus software, if you are lucky
- Social Engineering, YOU circumvent the AV (security control)

QUEEN'S UNIVERSITY BELFAST

Who is the weakest link? … you/me!

I am just one person working from home they wouldn't find me …

WRONG

You are now a valued target, with access to company assets!

You may:

- Be using personal devices for work with little/no security controls (e.g. anti-virus software)
- Be using new tools and platforms
- Have reduced access to IT support
- Make mistakes! … sharing with the wrong people …

QUEEN'S UNIVERSITY BELFAST

Hacking in the 1980s

Examples of real-life hackers

- 1981- ‘Chaos Computer Club’ (Germany)
- 1982- ‘The 414s’
- 1984- ‘Legion of Doom’, ‘Cult of the Dead Co
- etc.
- etc.
- 1994- Russian hackers stole $10 millions from Citibank
- etc.
- 2014- Worldwide global cost of cybercrime is estimated at $445 billion
- 2018- Worldwide global cost of cybercrime is estimated at $600 billion

QUEEN'S UNIVERSITY BELFAST

Password

Carbanak

- Dangerous combination of hackers and professional criminals
- A criminal gang that carries out Advanced Persistent Threat (APT) that often targets financial institutions (2014).
- Kaspersky lab believe them to be a Russian/UK Cyber Crime organisation
- The criminal manipulate their access to respective networks to steal money:
  - Manipulated databases to orchestrate an attack
  - ATMs – instruct ATMs to dispense cash, with money mules collecting money depositing the money to the criminal accounts.

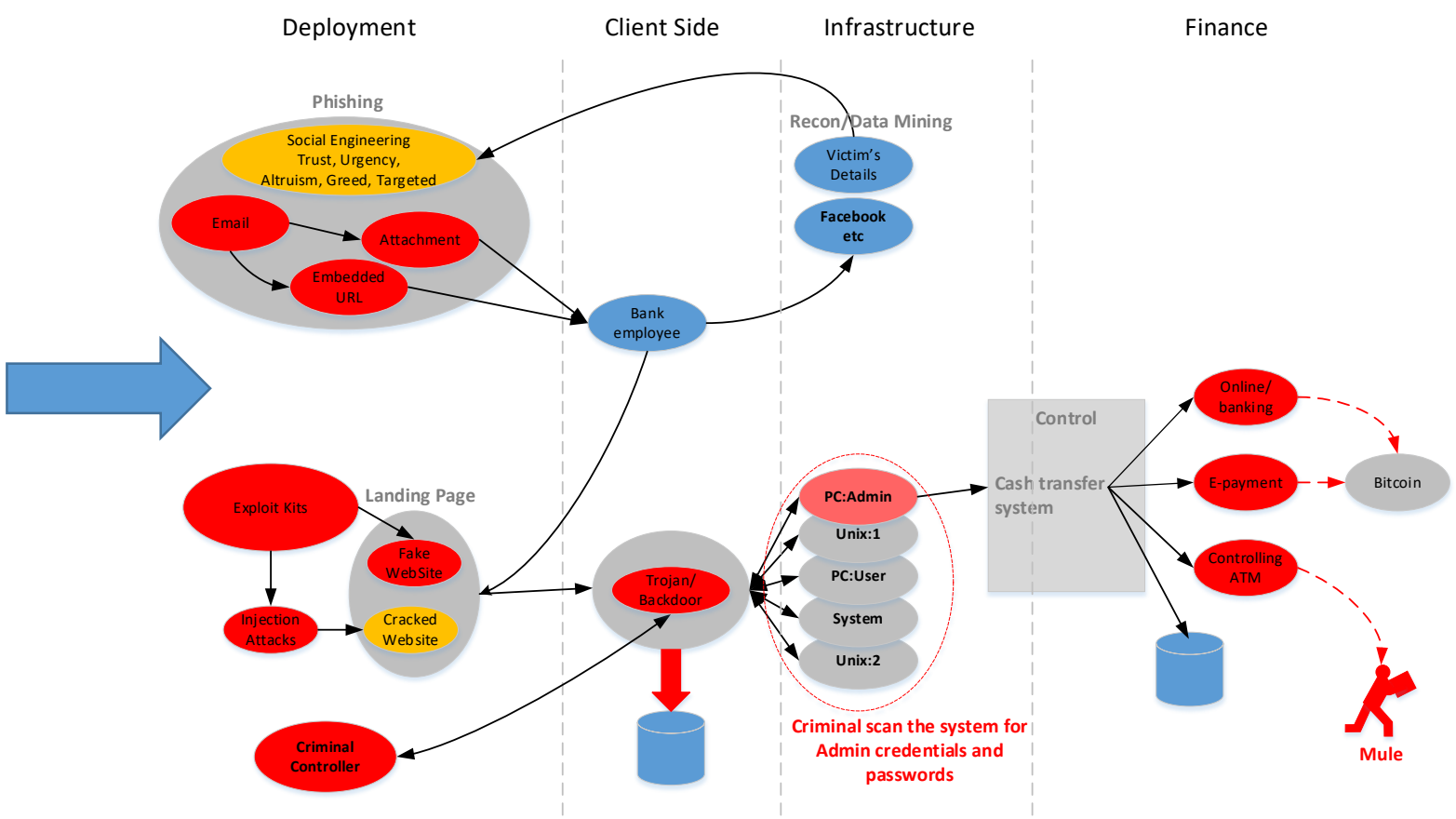
Carbanak creates file:

Family	File name	Size (bytes)	MD5
Trojan[Backdoor]/Win32.Carbanak	file.exe	404,992	a2643fe61f4b65704cfe1ebc55e2b301

Is **still active,** 5 Jun 2019

QUEEN'S UNIVERSITY BELFAST

Evolution of Attackers



QUEEN'S UNIVERSITY BELFAST

Password Hygiene

Users should:

- Create long, complex and unpredictable passwords
- Use unique password for each account
- Adhere to password policies: (aging, complexity rules, …)

Users often:

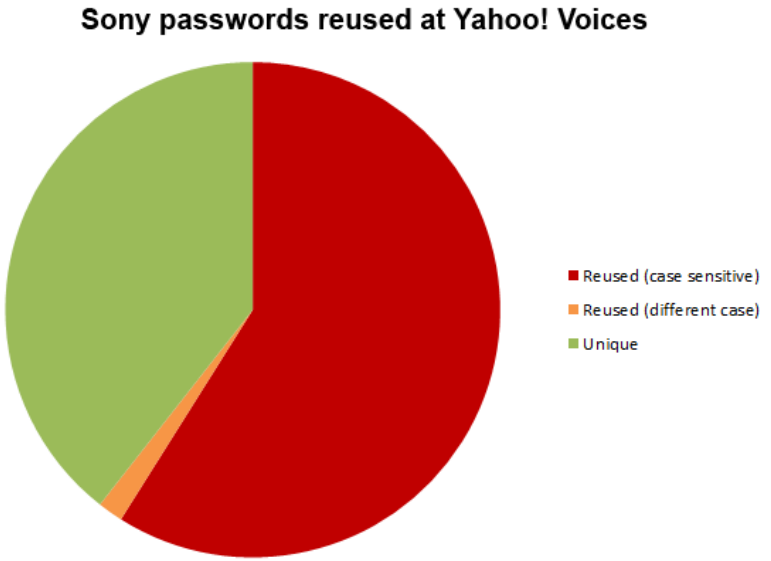
- Simple or common password that are easily found in reverse lookup tables
- Use the same password across multiple accounts, password reuse is a serious problem (password leaks)
- Don’t update of change their password even after a data breach

QUEEN'S UNIVERSITY BELFAST

Password Reuse

- Stats
  - 1% of passwords contain non-alphanumeric character
  - 4% contain two character types
  - 93% are 6 to 10 characters long

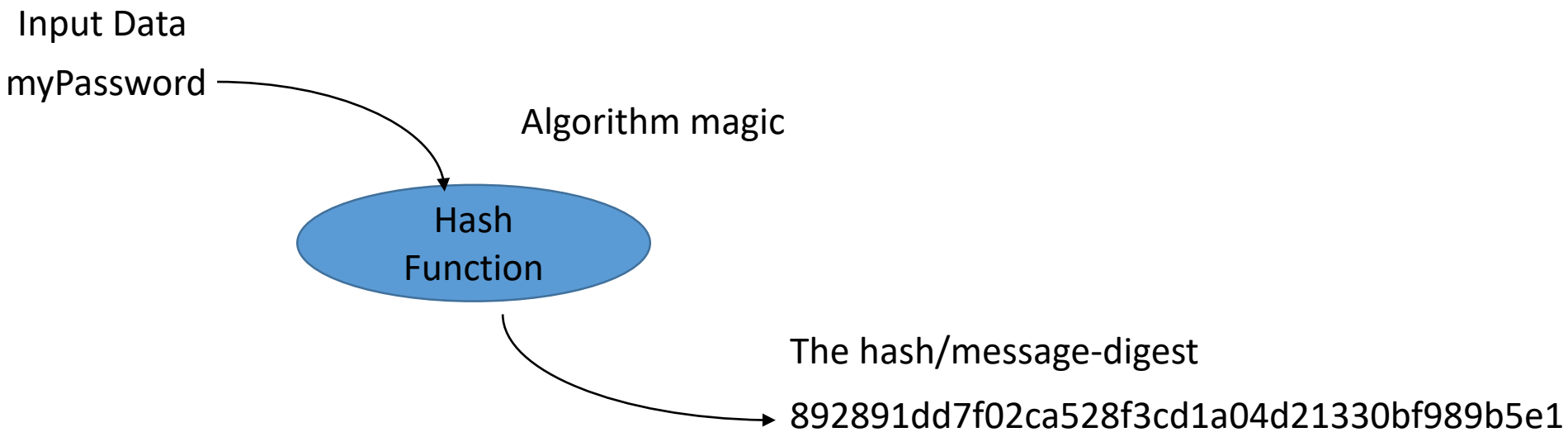
- A year after the Sony breach[1]:
  - *"59% of people were still using the exact same password on Yahoo! Voices."*
  - A further 2% of passwords only differed by case.



[1] https://www.troyhunt.com/what-do-sony-and-yahoo-have-in-common/

Hashing Algorithm

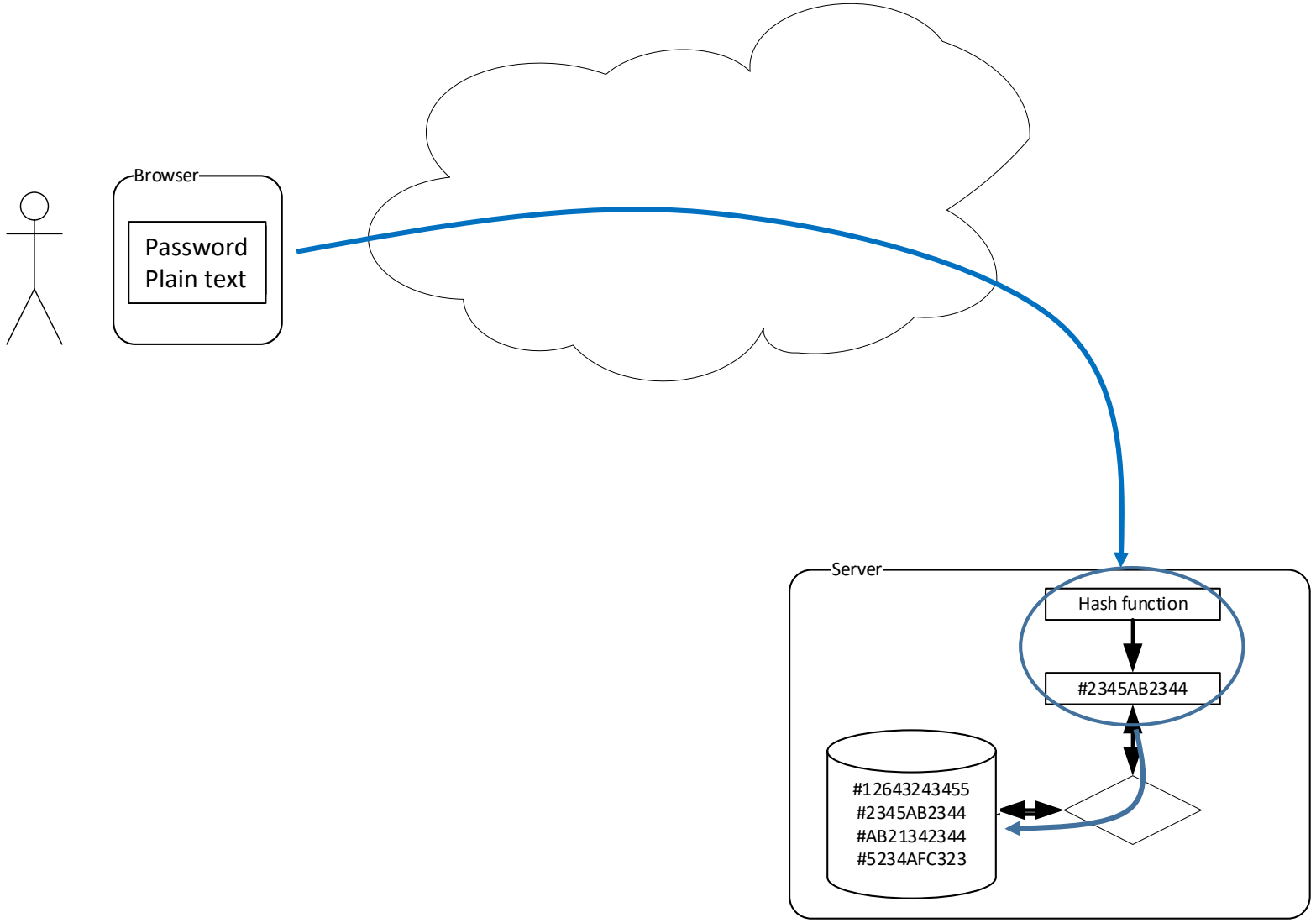
- Hashing algorithm is a complex mathematic function that transforms an input (string) in to a seemingly random sequence of numbers



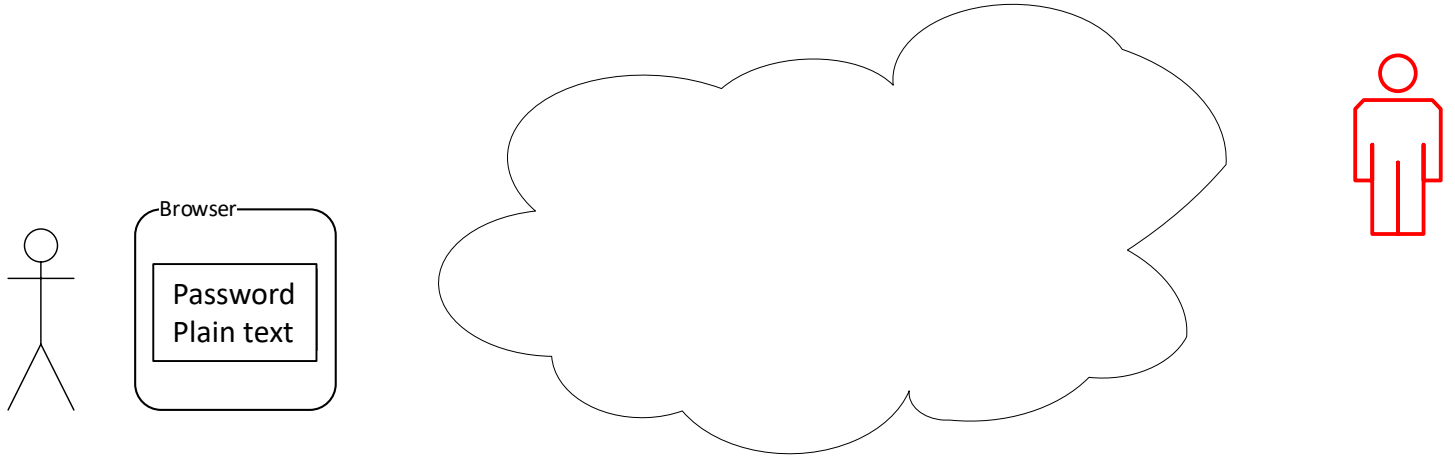
- **Encryption**: is often seen as a way of temporarily storing data until it is needed and then is unencrypted
- **Hashing**: is One-way -> you do not unencrypt (or un-hash) the hashed data

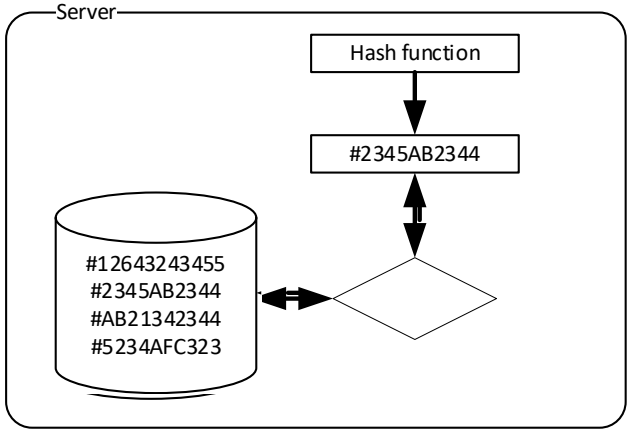
QUEEN'S UNIVERSITY BELFAST

Password Storage

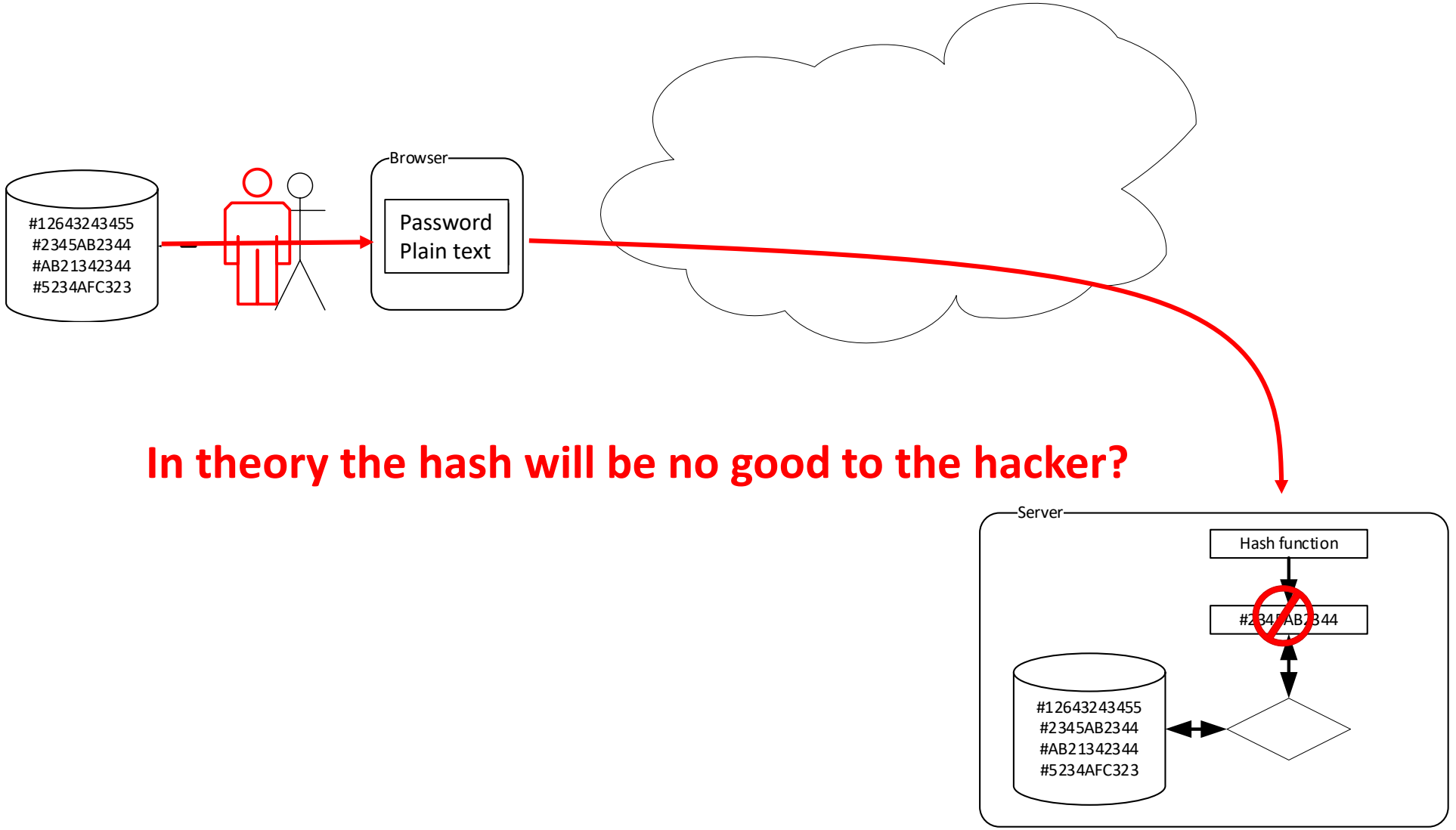


Password Storage





Password Storage



In theory the hash will be no good to the hacker?

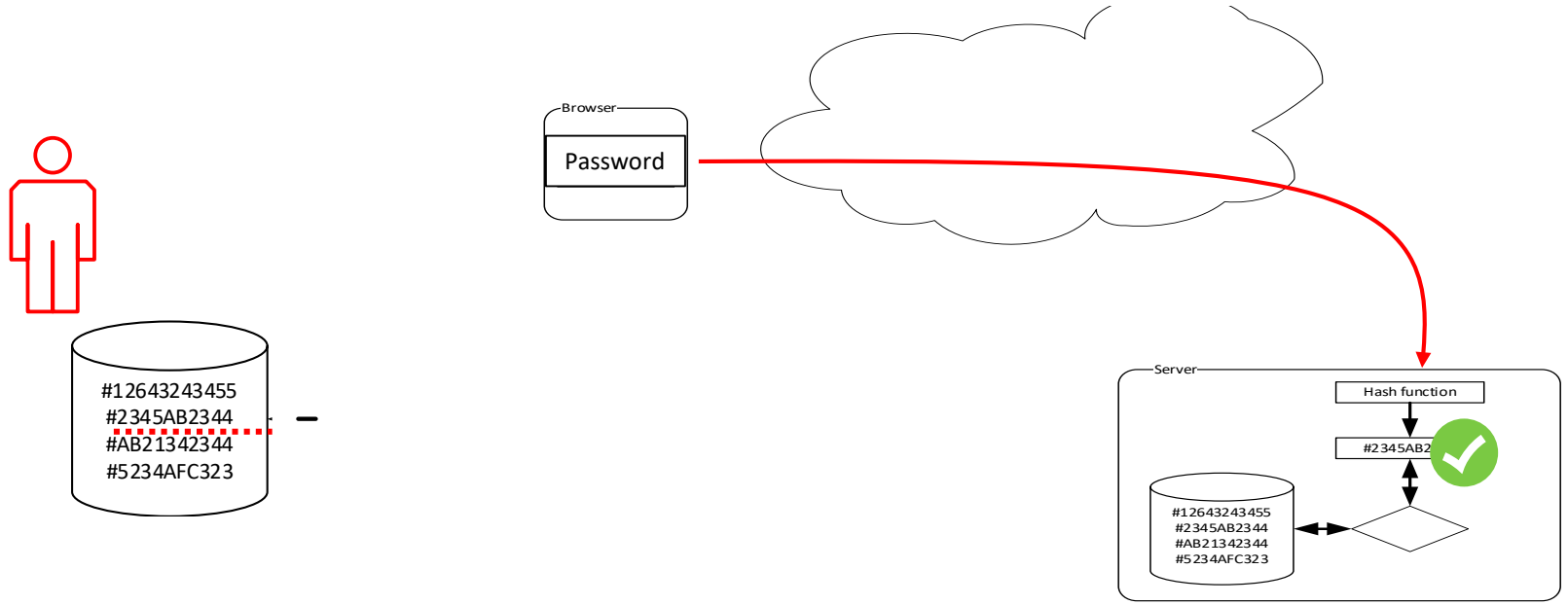
Reverse Lookup Table

Hash value	Original password
5413ee24723bba2c5a6ba2d0196c78b3ee4628d1	myPassword
7af2d10b73ab7cd8f603937f7697cb5fe432c7ff	Admin123
cd027069371cdb4f80c68dcfb37e6f4a1bdb0222	User123
521f17fee5fc459d7458c18b5220fc10412bed1e	myPa55w0rd
7d018bb3df0e523692845af1f27e992ce8a41650	mySecret
f8ec29af355cd3fb52ddaf5767134061a8d3ea13	tooManyPasswords

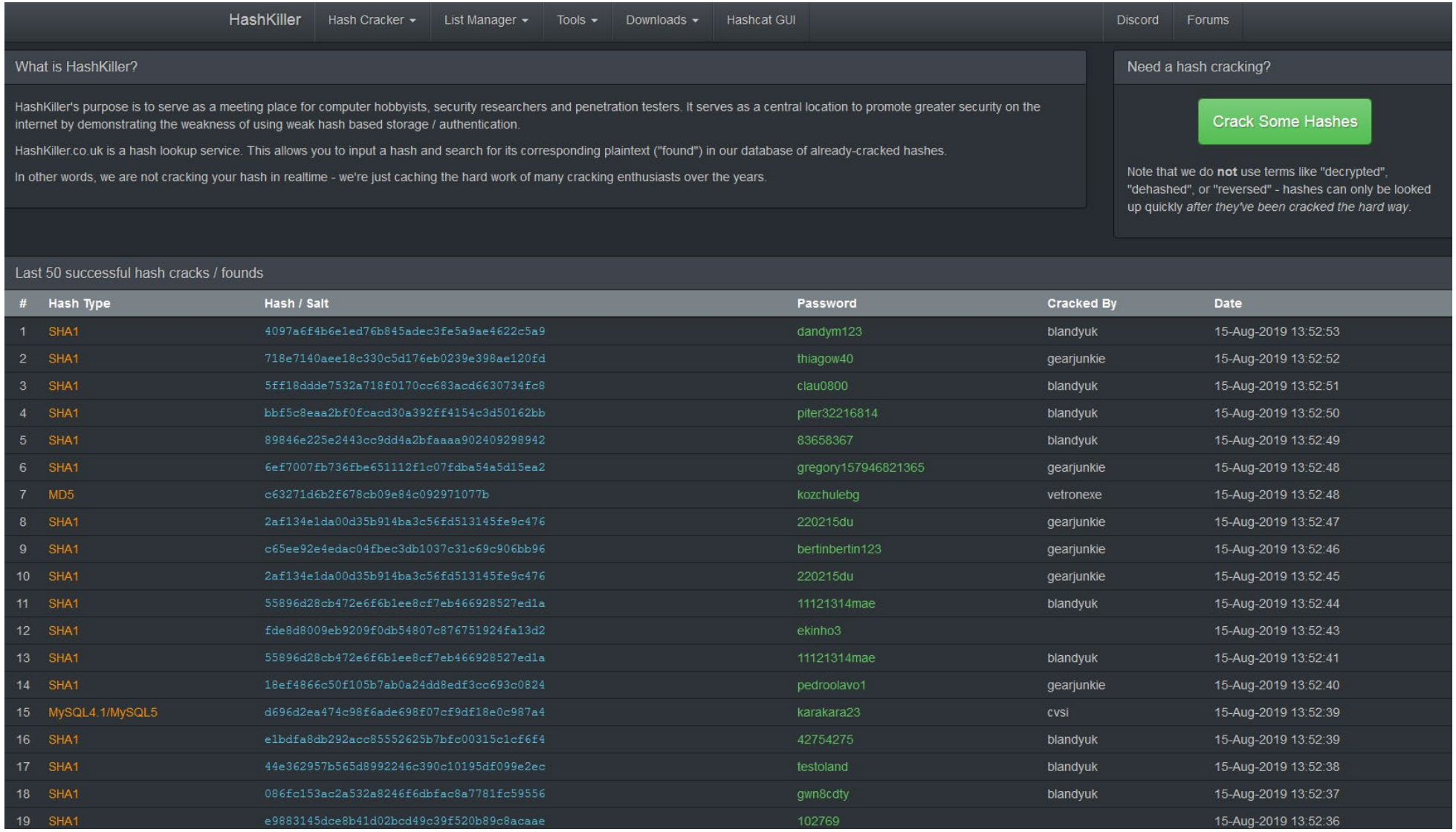
These tables can contain 100s millions of entries

Reverse Lookup Table

Hash value	Original password
5413ee24723bba2c5a6ba2d0196c78b3ee4628d1	myPassword
7af2d10b73ab7cd8f603937f7697cb5fe432c7ff	Admin123
cd027069371cdb4f80c68dcfb37e6f4a1bdb0222	User123
521f17fee5fc459d7458c18b5220fc10412bed1e	myPa55w0rd
2345ac23443412341a23232323232323232323	mySecretpassWord
f8ec29af355cd3fb52ddaf5767134061a8d3ea13	tooManyPasswords



Reverse Lookup Tables



HashKiller | Hash Cracker | List Manager | Tools | Downloads | Hashcat GUI | Discord | Forums

What is HashKiller?

HashKiller's purpose is to serve as a meeting place for computer hobbyists, security researchers and penetration testers. It serves as a central location to promote greater security on the internet by demonstrating the weakness of using weak hash based storage / authentication.

HashKiller.co.uk is a hash lookup service. This allows you to input a hash and search for its corresponding plaintext ("found") in our database of already-cracked hashes.

In other words, we are not cracking your hash in realtime - we're just caching the hard work of many cracking enthusiasts over the years.

Need a hash cracking?

Crack Some Hashes

Note that we do **not** use terms like "decrypted", "dehashed", or "reversed" - hashes can only be looked up quickly *after they've been cracked the hard way*.

Last 50 successful hash cracks / founds

#	Hash Type	Hash / Salt	Password	Cracked By	Date
1	SHA1	4097a6f4b6e1ed76b845adec3fe5a9ae4622c5a9	dandym123	blandyuk	15-Aug-2019 13:52:53
2	SHA1	718e7140aee18c330c5d176eb0239e398ae120fd	thiagow40	gearjunkie	15-Aug-2019 13:52:52
3	SHA1	5ff18ddde7532a718f0170cc683acd6630734fc8	clau0800	blandyuk	15-Aug-2019 13:52:51
4	SHA1	bbf5c8eaa2bf0fcacd30a392ff4154c3d50162bb	piter32216814	blandyuk	15-Aug-2019 13:52:50
5	SHA1	89846e225e2443cc9dd4a2bfaaaa902409298942	83658367	blandyuk	15-Aug-2019 13:52:49
6	SHA1	6ef7007fb736fbe651112f1c07fdba54a5d15ea2	gregory157946821365	gearjunkie	15-Aug-2019 13:52:48
7	MD5	c63271d6b2f678cb09e84c092971077b	kozchulebg	vetronexe	15-Aug-2019 13:52:48
8	SHA1	2af134e1da00d35b914ba3c56fd513145fe9c476	220215du	gearjunkie	15-Aug-2019 13:52:47
9	SHA1	c65ee92e4edac04fbec3db1037c31c69c906bb96	bertinbertin123	gearjunkie	15-Aug-2019 13:52:46
10	SHA1	2af134e1da00d35b914ba3c56fd513145fe9c476	220215du	gearjunkie	15-Aug-2019 13:52:45
11	SHA1	55896d28cb472e6f6b1ee8cf7eb466928527ed1a	11121314mae	blandyuk	15-Aug-2019 13:52:44
12	SHA1	fde8d8009eb9209f0db54807c876751924fa13d2	ekinho3		15-Aug-2019 13:52:43
13	SHA1	55896d28cb472e6f6b1ee8cf7eb466928527ed1a	11121314mae	blandyuk	15-Aug-2019 13:52:41
14	SHA1	18ef4866c50f105b7ab0a24dd8edf3cc693c0824	pedroolavo1	gearjunkie	15-Aug-2019 13:52:40
15	MySQL4.1/MySQL5	d696d2ea474c98f6ade698f07cf9df18e0c987a4	karakara23	cvsi	15-Aug-2019 13:52:39
16	SHA1	e1bdfa8db292acc85552625b7bfc00315c1cf6f4	42754275	blandyuk	15-Aug-2019 13:52:39
17	SHA1	44e362957b565d8992246c390c10195df099e2ec	testoland	blandyuk	15-Aug-2019 13:52:38
18	SHA1	086fc153ac2a532a8246f6dbfac8a7781fc59556	gwn8cdty	blandyuk	15-Aug-2019 13:52:37
19	SHA1	e9883145dce8b41d02bcd49c39f520b89c8acaae	102769		15-Aug-2019 13:52:36

Multifactor authentication

- Single-Factor
  Username/User ID and password to verify their identity.
- Two-Factor (2FA)
  Using a combination of two factors
    Something they know = PIN
    Something they have = ATM bank card; Online Mobile/SMS OTP;
- Multi-Factor (MFA)
  Uses multiple factors that are independent of each other
    Generate single sign-on passwords
    SMS – out of band SMS text message

QUEEN'S UNIVERSITY BELFAST

Summary of password failures

- Users and employees:
  - reuse the same password for most (if not all) of their accounts
    - 70% of employees reuse passwords at work[1]
    - Same password used across work and personal accounts
  - Use easy to hack passwords
    - criminals know that passwords are the weakest link, this is a high priority target
  - Privileged escalation
    - Even IT users reuse system admin passwords (50%)
  - Do not keep their passwords safe
    - Password rotation, users tend to reuse the same couple of passwords
- A Data Breach can destroy a business

Follow best practice guidelines: https://www.ncsc.gov.uk/section/advice-guidance/all-topics (**Use Strong Passphrases**)

[1]: 2018 Verizon Data Breach Investigations Report

QUEEN'S UNIVERSITY BELFAST

Danske Bank

Cyber Fraud and Scams

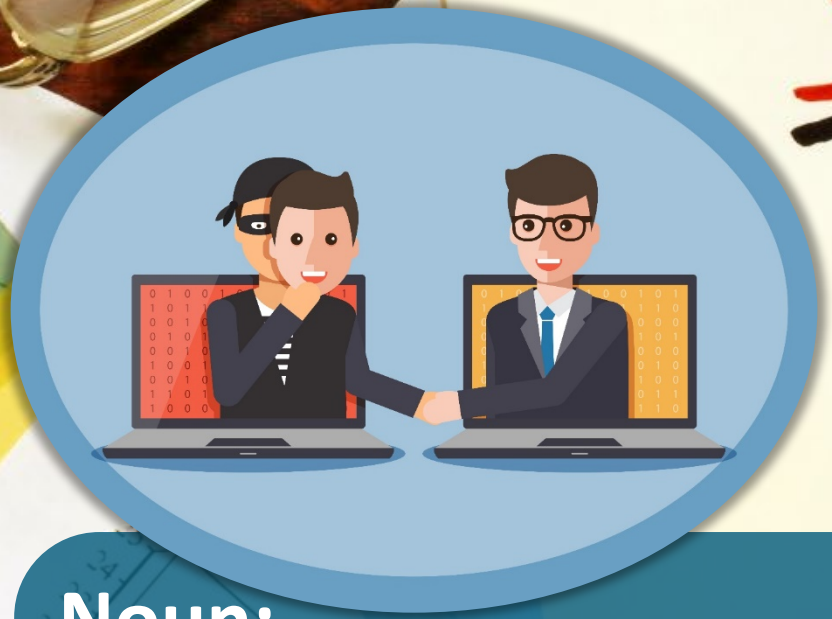
Chris leads a team of colleagues who are in the front line fight again fraud and scams. Together they provide support to customers who are victim to payment fraud, card fraud and cheque fraud.

Chris Wynne
Fraud & Cyber Crime Manager, Danske Bank

Fraud, Scams & Cyber Security

Chris Wynne
Fraud & Cyber Crime Manager

Danske Bank

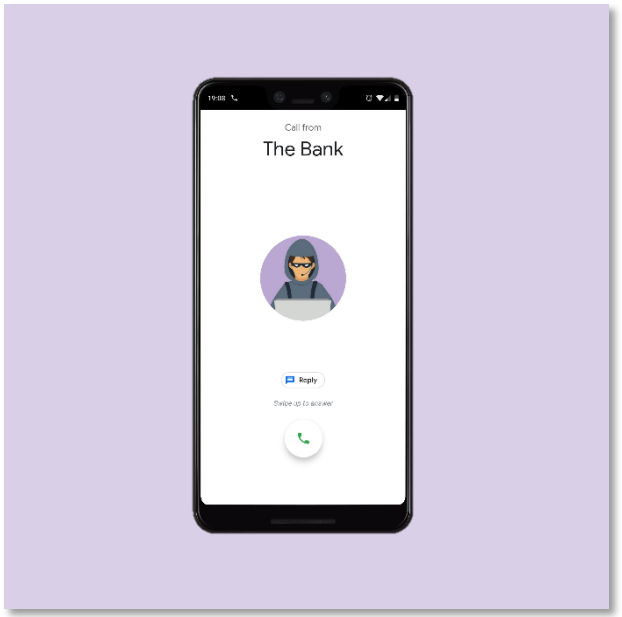


Noun:

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

So, what does ‘Social Engineering’ Look Like?

Phishing



Vishing

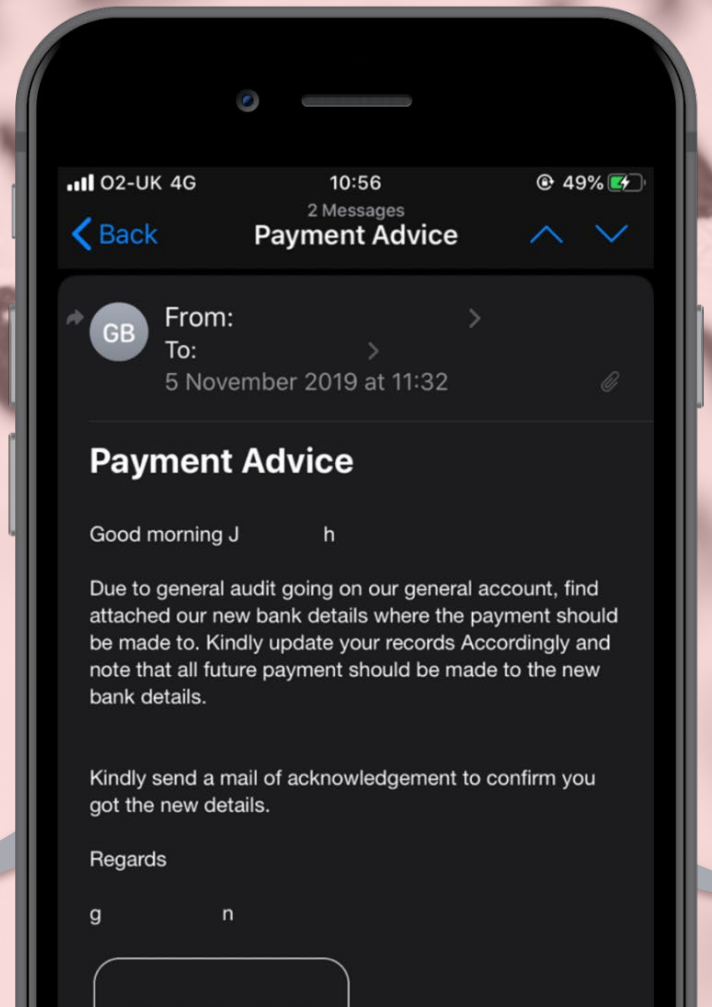
Smishing

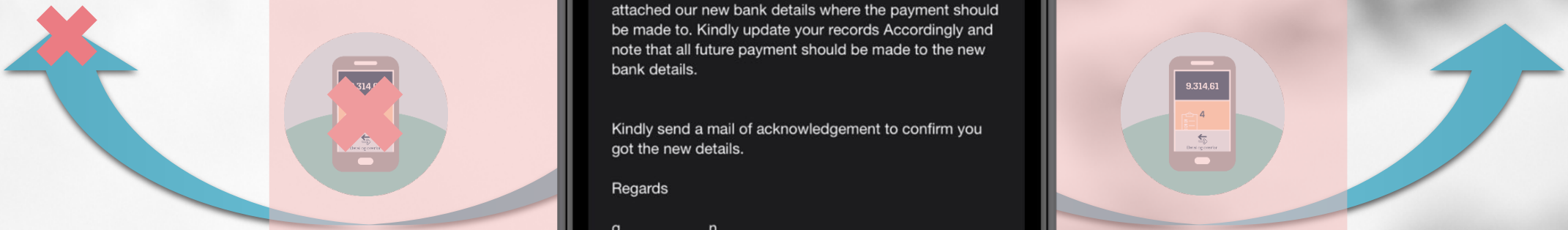
Invoice re-direction / Mandate fraud

You

Your Supplier

Criminal





Invoice re-direction / Mandate fraud

Belfast Telegraph DIGITAL

Hi 15°C | Lo 13°C Belfast | WEATHER

HOME NEWS SPORT BUSINESS ENTERTAINMENT LIFE CARS OPINION ARCHIVE

Northern Ireland | UK | Republic of Ireland | World | Politics | Brexit | Health | Sunday Life

Home › News › Northern Ireland

Email scams totalling almost £800,000 reported to PSNI in July

Chief Superintendent Simon Walls has warned that scammers will go to great lengths to trick their victims.

Simon Walls

scamwiseNI PARTNERSHIP POST OFFICE

£114 million

Lost during 2019 to Invoice Re-Direction Scams

Ireland › Irish News

Warning as Irish firms lose millions in sophisticated invoice scams

Two firms lost €650,000 recently in the so-called invoice redirection fraud

Mon, Nov 11, 2019,

Ronan McGreevy

THE IRISH TIMES

Mon, Sep 2, 2019

NEWS SPORT BUSINESS OPINION LIFE & STYLE CULTURE

Crime & Law | Brexit | Ireland | World | Politics | Social Affairs | Health | Education

We use cookies to personalise content, target and report on ads, to provide social medi

For more information see our Cookie Policy.

Dublin Zoo victim of €500,000 internet-based fraud by organised gang

Zoo tricked into paying invoices into bank account controlled by fraudsters

Belfast Telegraph

News Opinion Business Sport Life Entertainment Travel Sunday Life ≡ Sections

and UK Republic of Ireland World Politics Brexit Health Education Courts Obituaries Archive

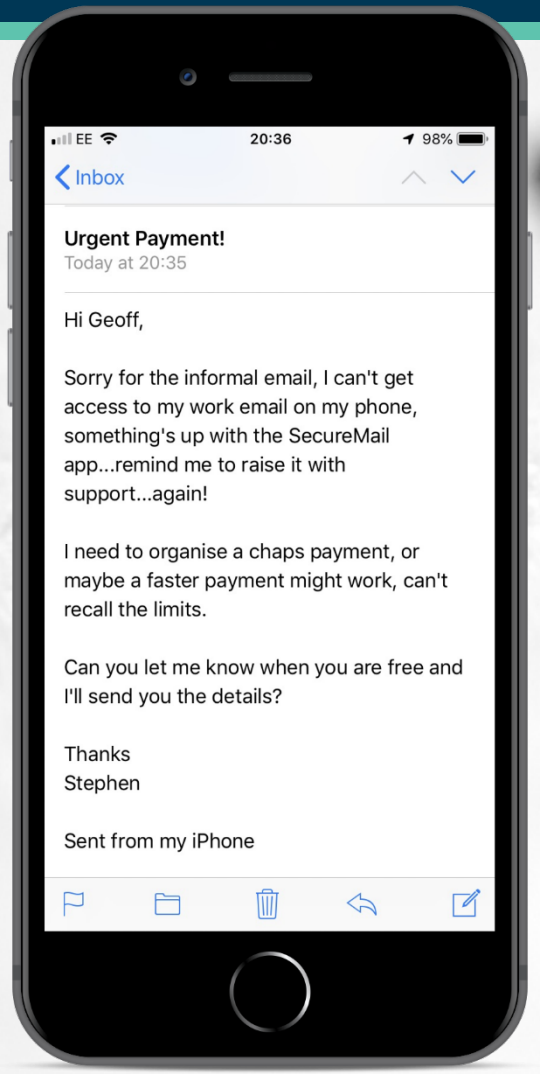
Irish firm sent 65,000 euro to fraudulent account in bid to buy PPE machine

Gardai in Waterford are investigating the scam with assistance from the Garda National Economic Crime Bureau.

IRISH BUSINESS REPORTS LOSSES OF €4.4M DUE TO INVOICE REDIRECT FRAUD

Source: UK Finance – Fraud the Facts 2020

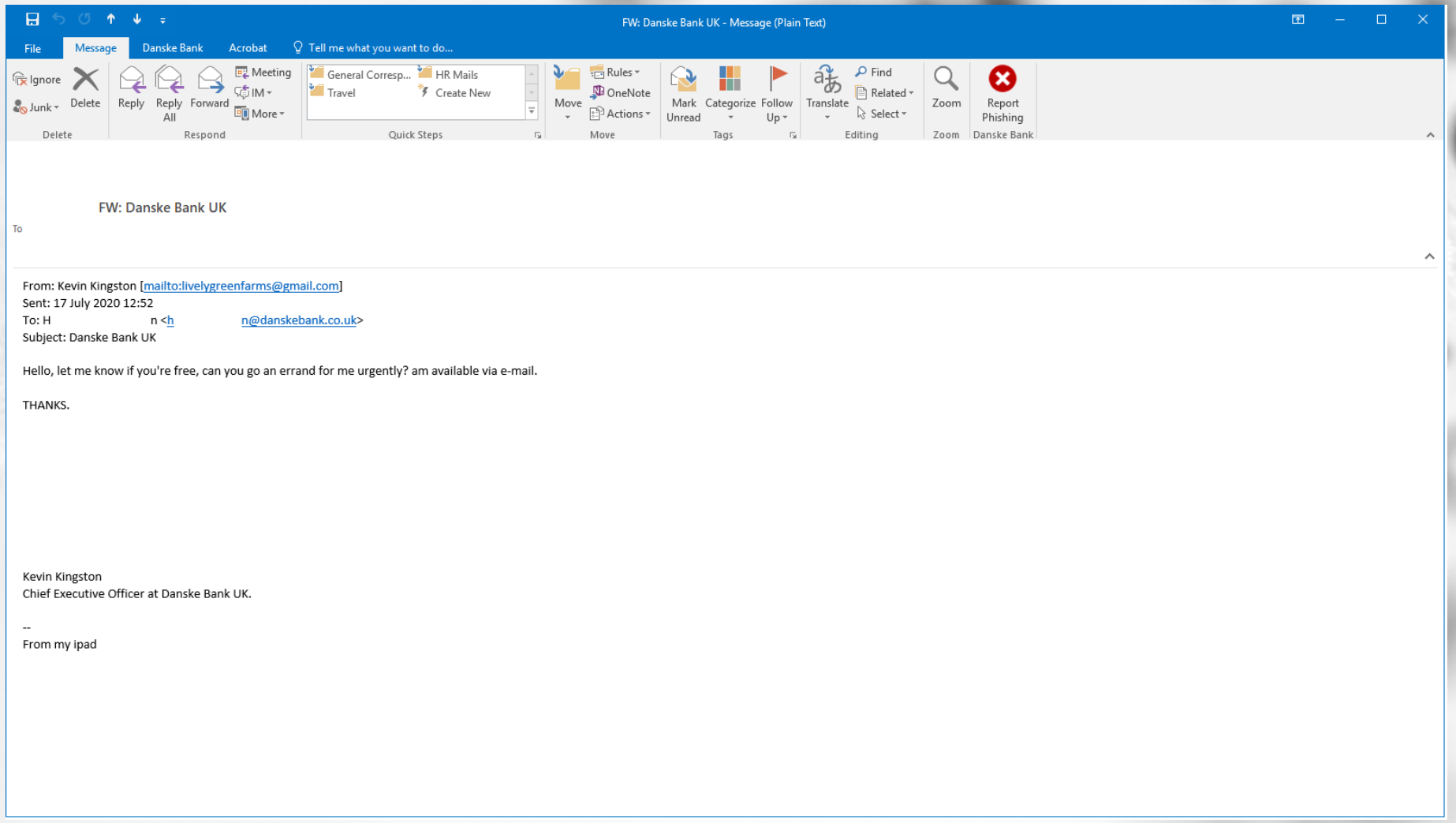
CEO fraud



- The fraudster will have done their homework, they will have an idea who is the correct person to target, i.e. who has the ability to make transfers.
- Typically they attempt to instil a sense of urgency about the payment being processed – about to board a flight, or need to seal a deal!
- A tendency to target key holiday periods has been noted, Easter, Twelfth Fortnight, Christmas etc. – when is it likely that the CEO/CFO/CRO/FD would be out of the office?
- They will either have a 'spoofed' e-mail address, or provide an excuse for not using their corporate mailbox. Can you spot the difference?

christopher.wynne@danskebenk.co.uk	christopher.wynne@danskebank.com.uk
christopher.wynne@danskebank.co.uk	christopher.wynne@dankebank.co
christopher.wynne@danksebank.co.uk	christopher.wynne@danskesbank.co.uk

CEO fraud



£17.9 million

Lost during 2019 to CEO Fraud

Source: UK Finance – Fraud the Facts 2020

How to keep it safe…

Keeping both yourself and your business safe does not need to be difficult

Here are some tips to help 'keep it safe'

Do you have controls in place and are they being followed?

For new payees or changes to existing ones - always verify account details with the intended beneficiary before sending any funds.

Ensure strong, unique passwords are used on all your accounts and enable two-factor authentication (2FA) where available.

Speak with you IT provider who can help.

Awareness is key – communicate these key risks amongst your colleagues.

Do you have a fraud adverse culture & are colleagues empowered to challenge?

Consider requests for payments for what they are.

If you are being rushed or panicked or something just does not stack up - all may not be what it seems.

Q&A

We will endeavor to answer as many questions as we can in connection with todays presentations.

A secure link to todays recording, presentations and information will be sent out later on today.