UWE Bristol University of the West of England
in association with National Cyber Security Centre
Department for Digital, Culture, Media & Sport
Academic Centre of Excellence in Cyber Security Education
UWE cyber Gold Award

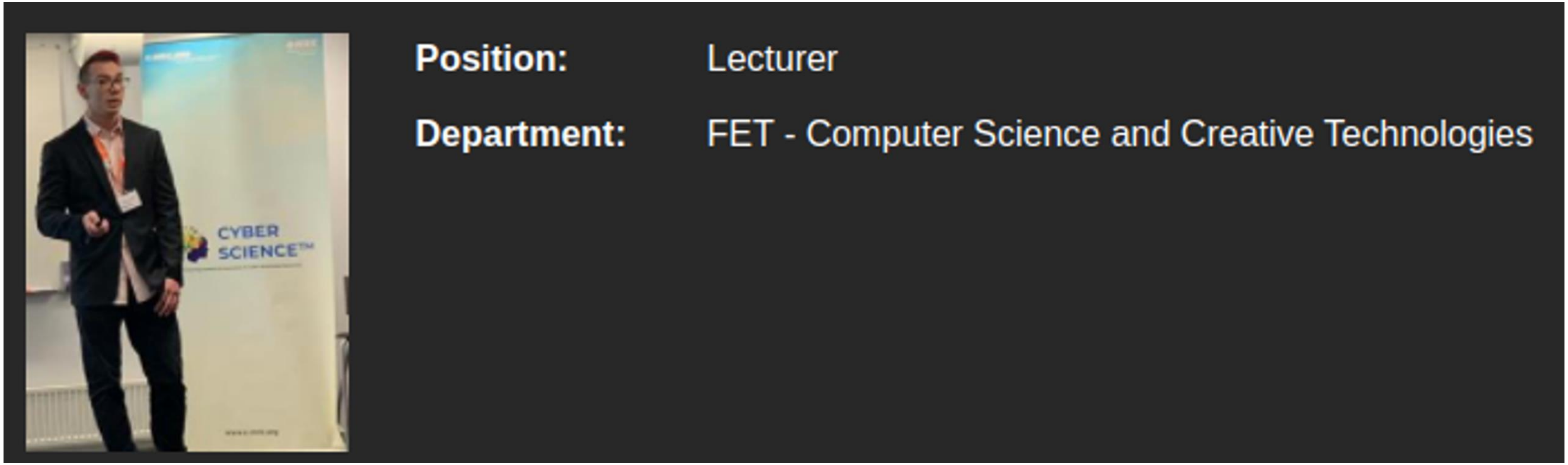
ACE CSE
TRAINING THE TEACHERS
Title in Progress

- **Alan Mills**
- **Lecturer in Cyber Security**
- **Alan.Mills@uwe.ac.uk**

- 2nd March 2022

Introduction

- Alan Mills - Alan.Mills@uwe.ac.uk



Position:	Lecturer
Department:	FET - Computer Science and Creative Technologies

Social Media, Digital Hygiene and Footprints

UWE cyber Gold Award

in association with National Cyber Security Centre

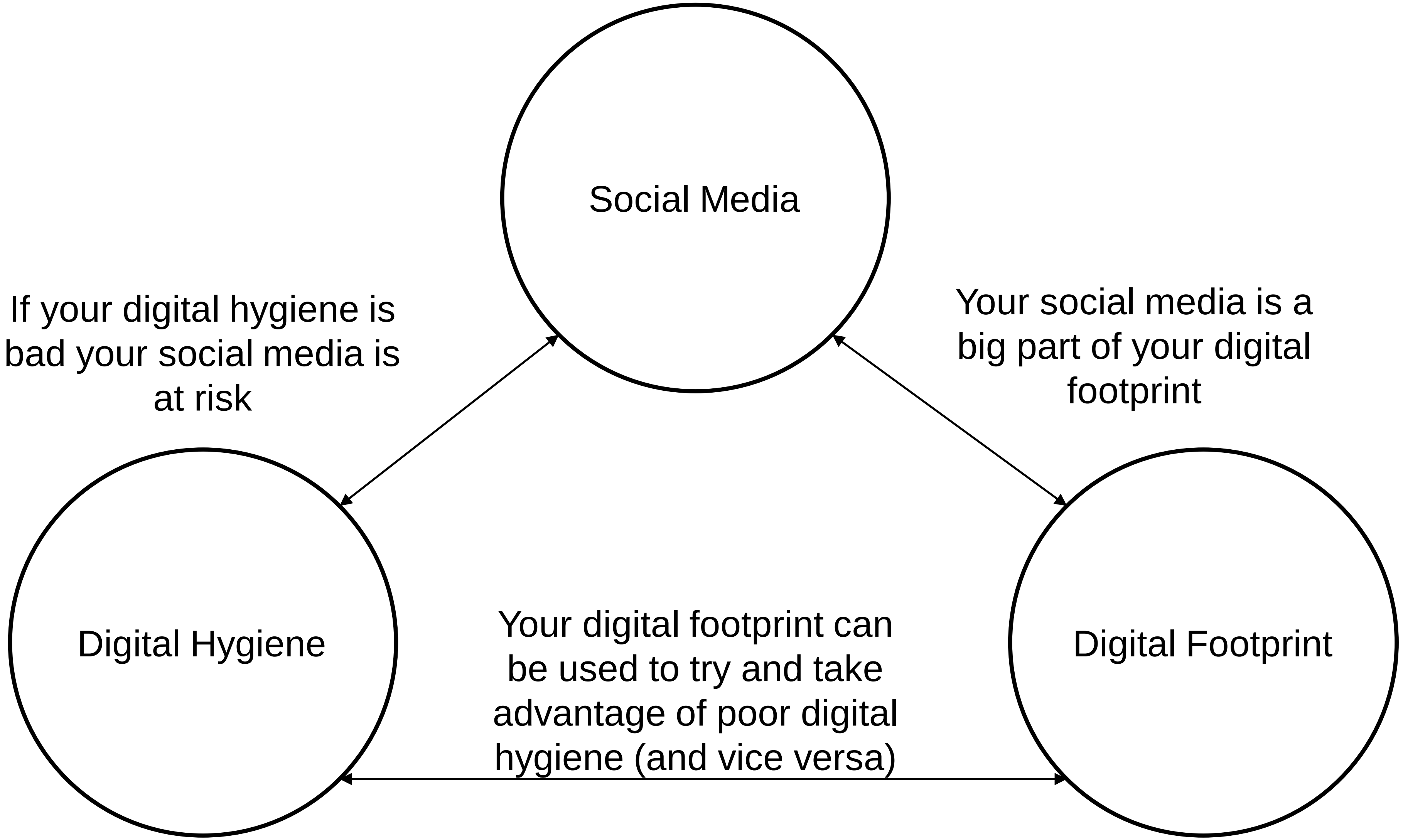
Department for Digital, Culture, Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

Introduction

- Social media, digital hygiene and footprints
- These have been put into the same session as they can all be tied into together

Introduction



Social Media

Digital Hygiene

Digital Footprint

If your digital hygiene is bad your social media is at risk

Your social media is a big part of your digital footprint

Your digital footprint can be used to try and take advantage of poor digital hygiene (and vice versa)

Social Media

- The easiest place to start – Everyone knows what this is

- Social media can be great – It also us to stay connected at a distance

- But it can also be mis-used:
  - Scammers
  - Phishing attacks
  - Malware
  - Sextortion
  - Cyber Bullying

- These issues aren’t unique to young adults – But they need to be told about them

Social Media

Young Adult Victims – Scams

- Before we go onto Social Media – I want to touch on scams in general
- There is a big assumption that online scams (and their victims) are largely the realm of the older generation
- This isn't always the case
- Sheildpay – A secure payment provider, posted (in 2018) that more 16-24 year olds were scammed then over 55s
- They also noted that the 16-24 year olds were losing more – An average of £613 compared to £337

Young Adult Victims – Scams

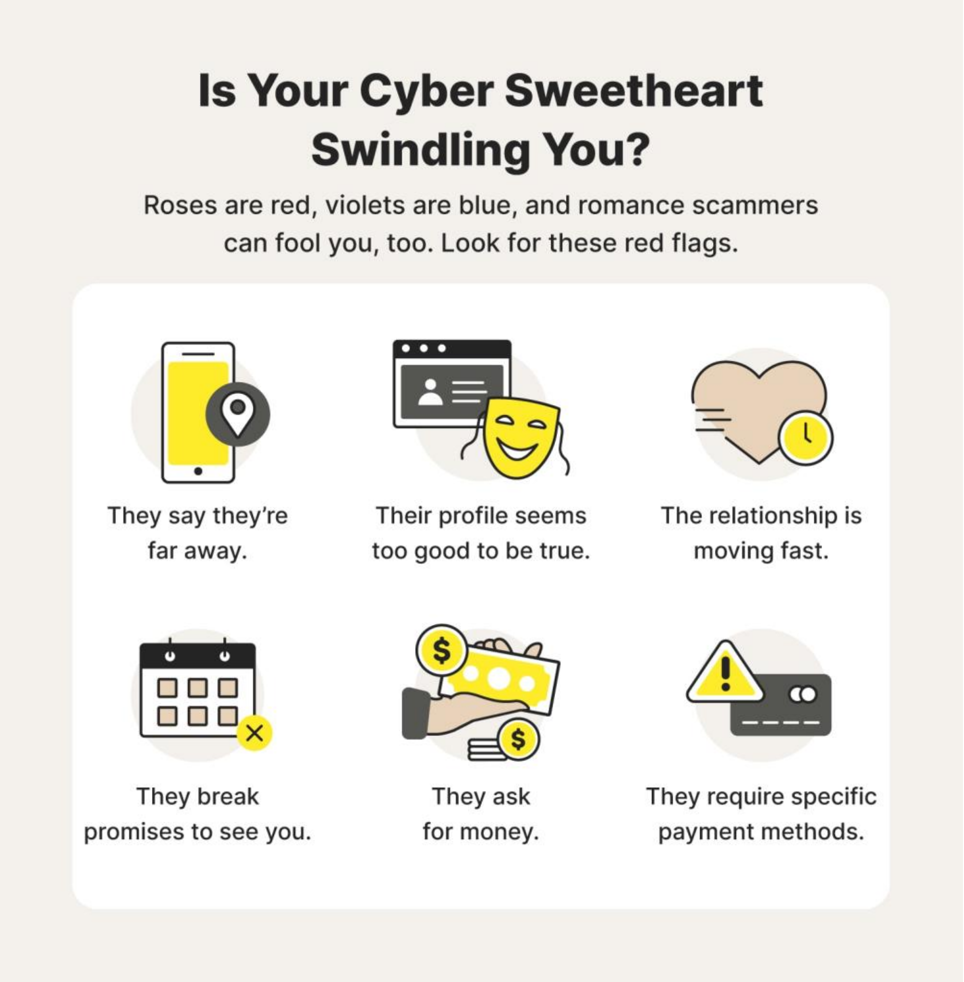
- A similar report found that those aged between 20 and 39 made up 40% of all scamming reports between Nov 2020 and Dec 2021
- The scams ranged from crypto currencies through to rent fraud and pyramid schemes
- Young adults are also falling victim to “push payment fraud”
- This is where you effectively transfer money from your account to a scammers
- In one instance the victim knew not to provide his password, One Time Passcode or allow them access to his machine
- But they didn’t ask for any of that – So they must be legit…. Right?

Social Media - Scams

- Romance scams
- Impersonation
- Job / Product scams
- Cryptocurrency

Social Media - Scams

- Romance scams are becoming more popular – They can also occasionally develop into sextortion (we will touch on this later)
- It’s catfishing rebranded
- These scams might start on social media
- They won’t always ask for money or photos
- Sometimes what they want is personal information which they can use



Is Your Cyber Sweetheart Swindling You?

Roses are red, violets are blue, and romance scammers can fool you, too. Look for these red flags.

They say they’re far away.

Their profile seems too good to be true.

The relationship is moving fast.

They break promises to see you.

They ask for money.

They require specific payment methods.

US Norton - Warning signs: Lies romance scammers tell

Social Media - Scams

- Impersonation scams

- These can have a lot of different variations but the scammer pretends to be someone else

- They might pretend to be someone you know or an authority figure
  - They might even be using their actual account

- They will likely try to get money out of you

Social Media - Scams

- In one instance for example a young women got a message from a friend and clicked on it

- It was a malicious link and her account was taken over

- The first she knew was when her friends and family let her know she was asking everyone on Instagram for money

Social Media - Scams

- Job / Product scams

- I’ve put both of these together for brevity – The end result is the same. Payment

- With job scams they will ask you to pay upfront for training or qualifications etc

- With the product scams you simply don’t get the product you did pay for
  - The use of things like FaceBook market-place can make these harder to spot

- If you pay for something that you don’t receive you can claim it back (depending on how you paid)

Social Media - Scams

- Cryptocurrency scams
- We could almost spend an entire session on these
- Bogus sites
- Fees and charges for withdrawing money
- Impersonation scams pushing the above

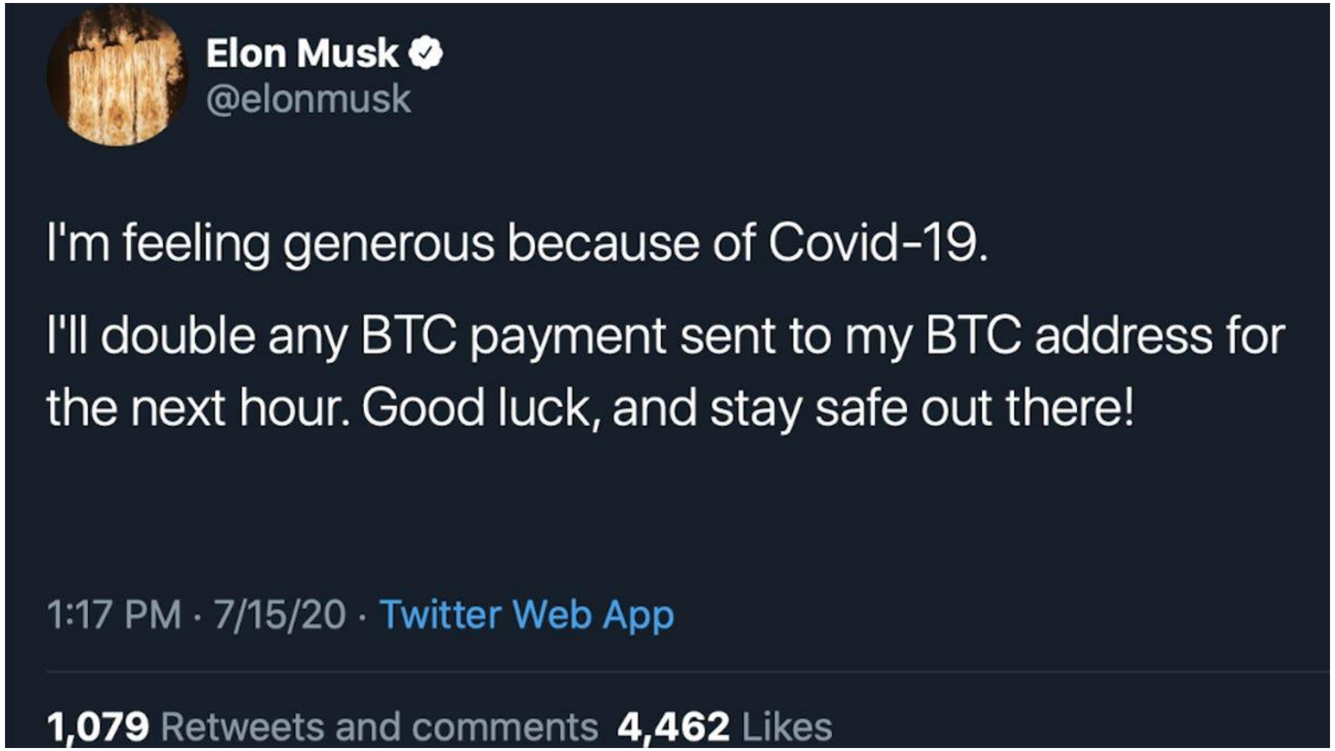
Social Media - Scams

- Cryptocurrency scams

- In 2020 a co-ordinated scam took place which was launched from multiple hacked social media accounts

- In a similar vein social media accounts can be created which impersonate well known investors

- These are then used to scam people



Elon Musk
@elonmusk

I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to my BTC address for the next hour. Good luck, and stay safe out there!

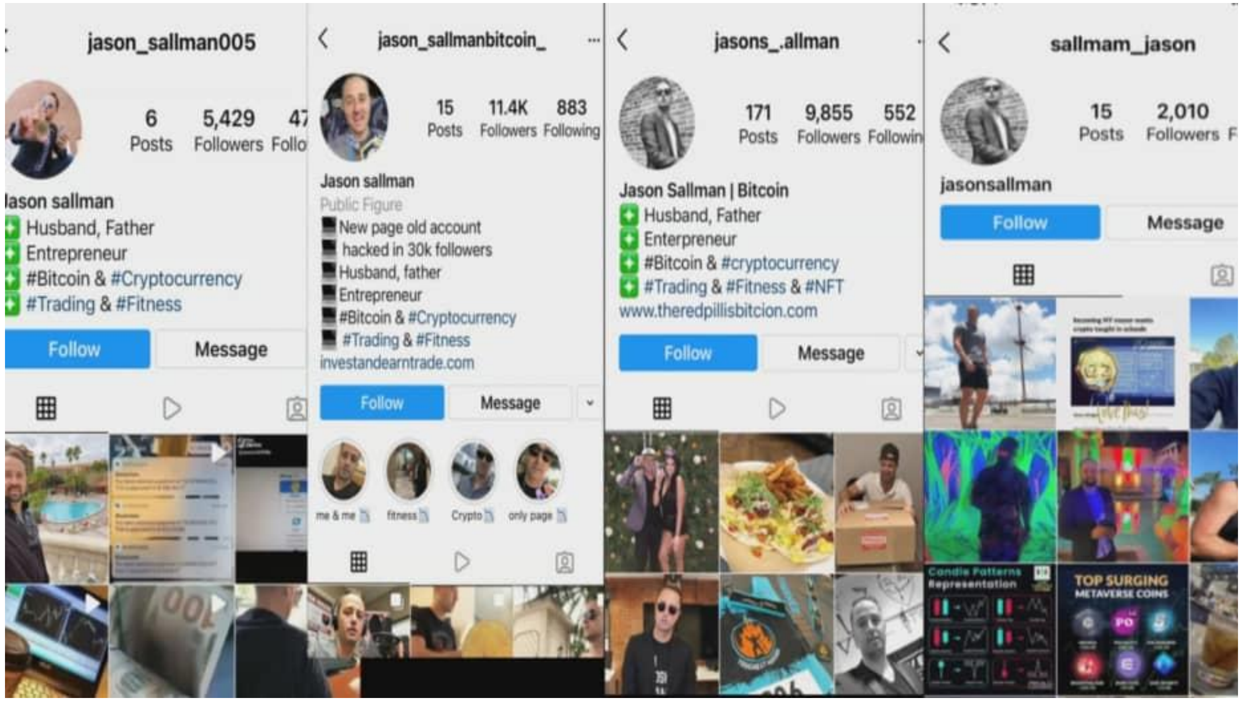
1:17 PM · 7/15/20 · Twitter Web App

1,079 Retweets and comments 4,462 Likes

CNET - The Bitcoin scam as it appeared on Elon Musk's Twitter feed.

Social Media - Scams

- Cryptocurrency scams - Impersonation
- For example one story about someone named Jason Sallman shows multiple fake accounts have been created with his name
- In one instance a victim of one fake account lost $20,000
- Jason Sallman himself has been getting threats from the victims!



jason_sallman005

lason sallman
Husband, Father
Entrepreneur
#Bitcoin & #Cryptocurrency
#Trading & #Fitness

jason_sallmanbitcoin_

Jason sallman
Public Figure
New page old account
hacked in 30k followers
Husband, father
Entrepreneur
#Bitcoin & #Cryptocurrency
#Trading & #Fitness
investandearntrade.com

jasons_.allman

Jason Sallman | Bitcoin
Husband, Father
Entrepreneur
#Bitcoin & #cryptocurrency
#Trading & #Fitness & #NFT
www.theredpillisbitcoin.com

sallmam_jason

jasonsallman

CNBC - Jason Sallman said scammers are stealing his photos to create accounts that impersonate him on Instagram.

Social Media - Phishing

- Some aspects of Social Media Phishing (SMP) we’ve already covered – Like links from friends or known accounts
- In other cases they might be links from apps or platforms to update your details
- In some cases they might be seemingly innocent friend requests, profiles or messages
- The impact from being phished can vary
  - They might immediately hijack your device or account
  - They might ask for personal information or details
  - They might install spyware / malware…

Social Media - Malware

- Phishing is a common way malware can be propagated, but not the only way

- Much like with emails social media has developed its own spam content
  - You only have to click once

- Some malware will also masquerade as legitimate apps
  - People may download them of their own accord
  - People might be asked to download recommended apps

- In some cases the malware can even masquerade as an image or overlay on social media buttons

Social Media - Sextortion

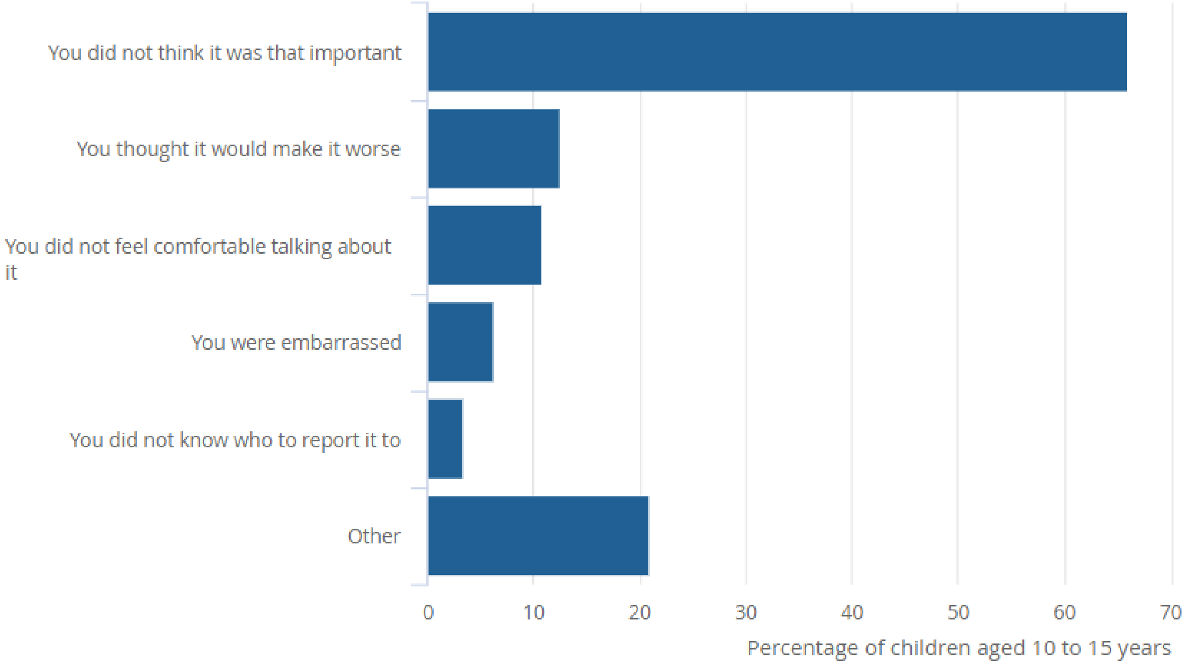
- Sextortion isn’t new – But it is on the rise
- It also isn’t just targeting women – In one case a young man was victim to an attempt that started on Instagram
  - They tried to get the victim to pay £1,500 to stop intimate videos of him being shared
- Subjects like this are – touchy
- But if people aren’t aware or warned then they can’t be smart about it

Social Media – Cyber Bullying

- Bullying is sadly something that does, and will continue to, impact people
- Social media has opened up a new avenue for communication and bullying / harassment
- 19% of children aged 10-15 in England and Wales have experienced cyber bullying (2020 government report)
- Of those who experienced cyber bullying, 72% also experienced in person bullying during school hours

Social Media – Cyber Bullying

- The range of cyber bullying can vary from targeted insults and threats to being excluded or rumours spread
- The impacts of cyber bullying can vary – But can include extreme emotional impact through to feeling suicidal
- Despite the impact 26% of 10-15 olds impacted didn’t report cyber bullying



Office for National Statistics – Reasons behind not reporting cyber bullying

Social Media – Safe usage

- Ultimate a lot of what can be done to ensure safe social media usage could be referred to as “common sense”

- It is also the same advice we’d offer for almost any internet based interaction:
  - Install (and use!) an anti-virus
  - Multi-factor authentication
  - Check links before clicking on them – VirusTotal
  - Check reviews, feedback and ratings
  - Check profiles
  - Pause and think – Always err on the side of caution
  - Don’t share something you wouldn’t want made public
    - Don’t show your face at least!
- +7926

Social Media – Safe usage

- If the worst happens – Don’t panic!

- If you’re scammed – Try and get your money back (citizenadvice)

- If you suspect malware has been installed – Disconnect the device from any and all networks

- If you suspect an account has been compromised – Report it
  - Change the password(s)

Social Media – Safe usage

- If someone tries to extort you – Go to the authorities
  - Payment will not ensure it / they “go away”
  - Do not do what they ask!

- Cyber bullying – If you suspect a student is a victim there are multiple resources:
  - The NSPCC helpline on 0808 800 5000 or by emailing help@nspcc.org.uk
  - Childline on 0800 1111
  - Local child protection services

Digital Hygiene

Digital Hygiene

- Digital Hygiene is a (hopefully) common phrase
- It is basically a focus on safe and sensible practices to keep your digital life "healthy"
- A often used phrase is:
  - "*Treat your passwords like your underwear. Change them regularly and don't share them*"
- Concepts like this are good advice – But they aren't the extent of digital hygiene

Digital Hygiene - BuzzFeed

- Sites like BuzzFeed are constantly farming people's information

- Various quizzes and questionnaires are a great way to get you to give them your personal information
    - Chances are Harry Potter didn't need to tell the sorting hat his first pets name

- While this information is often utilised for advertising and product placement it can also be mis-used

- For example there's a good chance that "Name of your first pet" is both a security question and a BuzzFeed quiz question

Digital Hygiene – Social Media

- The same is true for what you share on social media
- If your profile tells everyone everything it makes it much easier to try and answer security questions
- Especially if it’s a public profile
- It also makes it much easier for people to target you with impersonation based scams / attacks

Digital Hygiene – Social Media

[How private is your personal information? - YouTube]

Digital Hygiene – Credentials

- Passwords or passphrases are naturally a big consideration
- We want to ensure they are hard to guess or crack
- We also don't want to re-use the same password for everything
- No matter how secure we might think it is
- A data breach for example will expose both the secure password and the associated email address or login

Digital Hygiene – Devices

- It is now common for people to treat their phones in a similar fashion to their computers
- Work, emails, internet browsing and entertainment
- Unfortunately they often don't treat device security the same on both
- Most laptops or computers will have antivirus protection – Especially if it is a work computer
- We need to treat our phones the same way

Digital Hygiene – Public WiFi

- Internet usage and availability are now almost considered the same way as water and energy
- It is now so common for WiFi to be made available that we don't check for it – We just assume
- Sadly public WiFi is not always the most secure
- VPNs and / or the use of TOR networks can help with that
- Being aware of it and avoiding any sensitive usage can help even without VPNs or TOR

Digital Hygiene – Staying Clean

- Privacy settings
- Does everyone / anyone *really* need to know everything?
- Vary your security questions and answers if possible
- Password managers
- Antivirus and endpoint protection
- Public WiFi awareness

Digital Footprint

Digital Footprint

- Our digital trace – Can also be considered as how much evidence of our lives or existence is online?
- Some people by design have a large digital footprint
- Some people by accident
- Some due to malicious circumstance

Digital Footprint

- Once something has been made available on the internet it is almost impossible to have it removed
- Images and posts made years ago can still be found, shared and used – Potentially against the person who posted them
- Even if something is shared only briefly – If it's long enough for someone to take a screenshot it's long enough to be immortalised

Digital Footprint

- Because of this malicious actors will try and extort or blackmail people if they have gained access to someone's account
- They might threaten to post / leak images or videos
- They might threaten to make statements or carry out actions while masquerading as you
- They are attempting to use your digital footprint against you

Digital Footprint

- Things like this are not made any easier by the fact that our digital footprint and digital identity are becoming more important
- Employers will often look at a person's digital footprint
- Background checks will flag any online behaviour that might be deemed undesirable
- The importance of your digital footprint makes it a viable target

Session 1 - Overview

- Social media, digital hygiene and footprints
  - *If you tell BuzzFeed your security answer(s) chances are they aren't secure*
  - *If you use the same password for multiple accounts it only has to be compromised once*
  - *Do you use your phone as much as your computer? Which one has an Anti-Virus?*
  - *Check reviews, ratings and feedback before downloading or buying*

SUMMARY

Summary

- **Social Media**
  - *Scams*
  - *Phishing*
  - *Malware*
  - *Sextortion*
  - *Safe Usage*
- **Digital Hygiene**
  - *Public Information*
  - *Credentials*
  - *Devices*
  - *Public Networks*
  - *Staying Clean*
- **Digital Footprint**
  - *TBC*

Next Session

- OS Reporting, Intelligence and Verification

Q&A

Links

- https://www.credit-connect.co.uk/news/consumer-collections/young-people-most-likely-to-be-victims-of-online-fraud/
- https://uk.finance.yahoo.com/news/scams-young-people-fraud-victim-cryptocurrency-which-000140441.html?guccounter=1&guce_referrer=aHR0cHM6Ly9zZWFyY2guYnJhdmUuY29tLw&guce_referrer_sig=AQAAAUZVb7ptcP3VzucpZV8F42QYY-xo9je5QWhuLjqEJXperhGoVWU_cgzAlP4mDBjd_CfH43gy5rKe48fVGNZuraR_5geCh9fd8m2yZbWAdV0ufSK9e7fq5H7feOivu2EsTvavRY8MUBggHoxafpHvmE45P6xEtFvyeocr3JWl9Ra
- https://www.bbc.co.uk/news/business-58499998
- https://us.norton.com/internetsecurity-online-scams-romance-scams.html#
- https://www.cbsnews.com/miami/news/young-adults-social-media-scams/
- https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/onlinebullyinginenglandandwales/yearendingmarch2020
- https://cybercrew.uk/blog/cyberbullying-statistics-uk/
- https://www.citizensadvice.org.uk/consumer/scams/check-if-you-can-get-your-money-back-after-a-scam/
- https://www.dnaindia.com/mobile/report-dangerous-malware-found-on-8-google-play-store-apps-that-steal-your-data-2969495

Links

- https://www.difesaesicurezza.com/en/defence-and-security/beware-of-memes-on-social-media-cybercrime-uses-them-to-hide-malware/
- https://www.galaxkey.com/blog/social-media-icons-hide-skimming-malware/
- https://inews.co.uk/inews-lifestyle/reports-sextortion-soaring-uk-how-to-stay-safe-1704431
- https://digitalhygiene.net/
- https://www.gov.uk/government/consultations/digital-identity

Required software

- If any