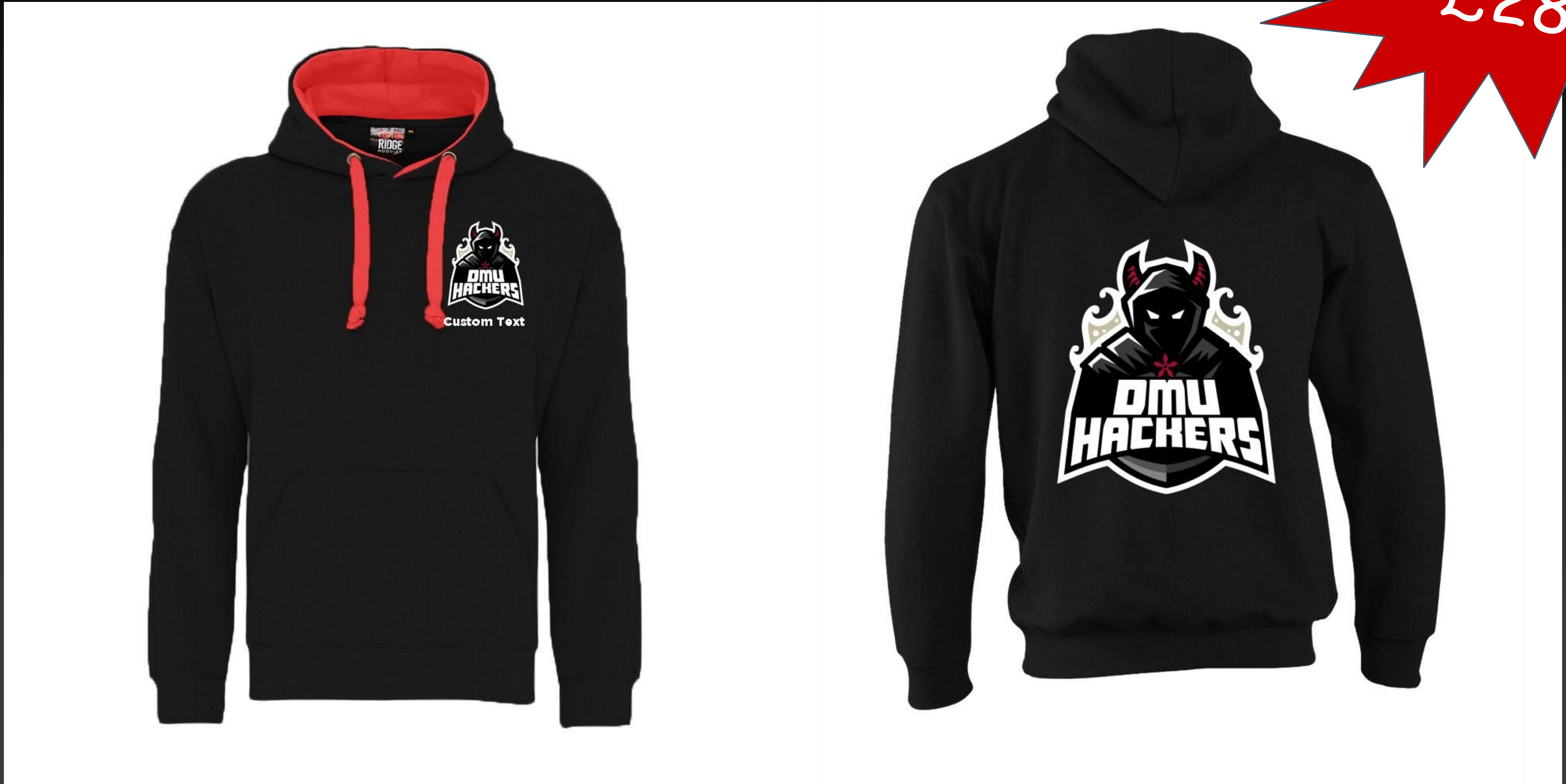
OMU
HACKERS

Announcements

- Welcome back !!
- CTF back on Wednesday
- Committee nominations
- SIGINT pwnEd CTF
- And also…

Hoodies

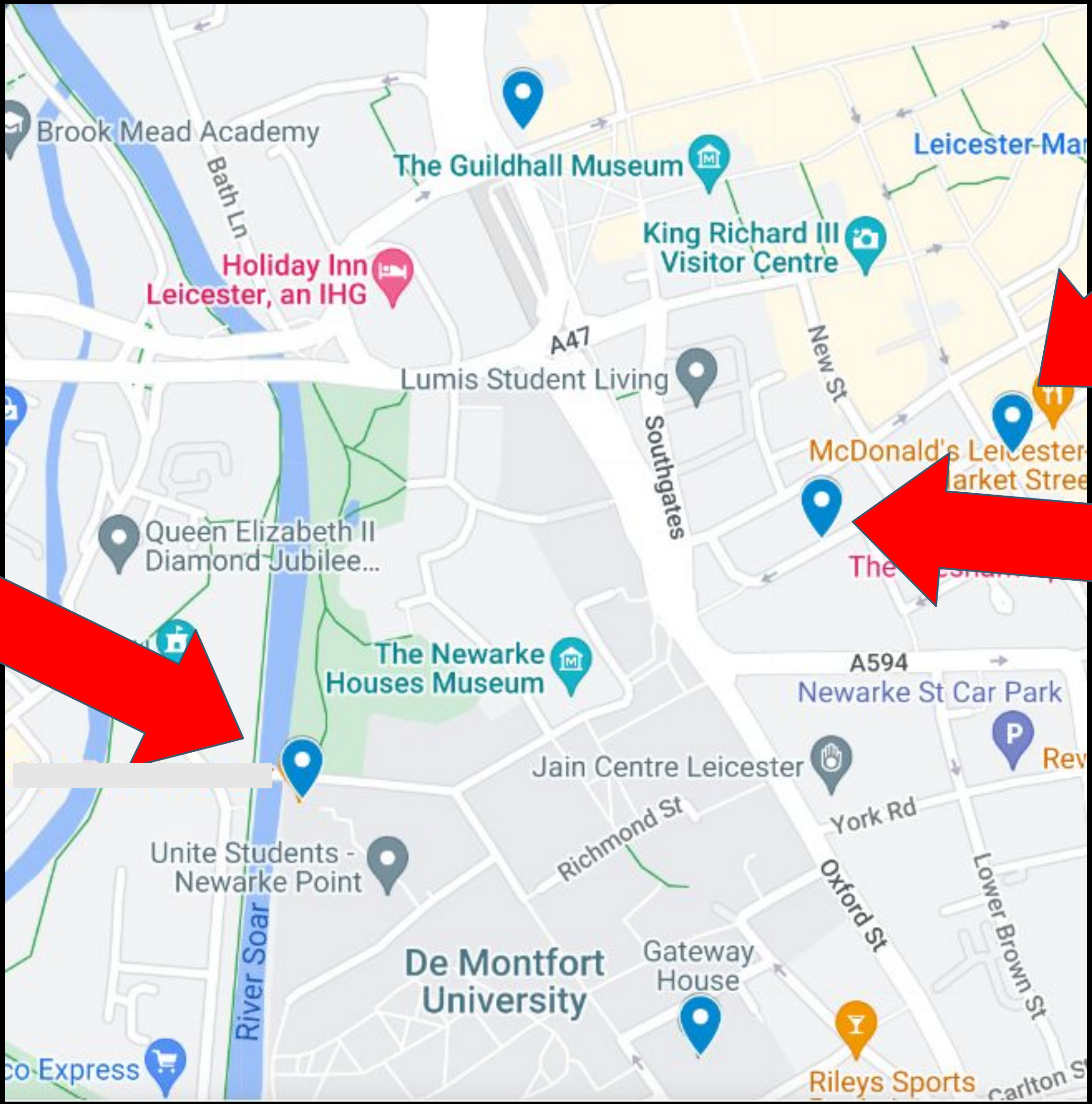
£28



DMU HACKERS

Social

THE SOAR POINT



FIREBUG
BAR . VENUE . FOOD

oddbar

DMU HACKERS

hackers.dmu

@dmuhackers

DMU HACKERS

Social Engineering

Don't do illegal shit

What is Social Engineering?

"Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables."

What is Social Engineering?

- Range of malicious activities accomplished through human interactions
- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information
- It exploits humans rather than vulnerabilities in tech

The Psychology Behind Social Engineering

Reciprocity

Commitment/Consistency

Social Proof

Authority

Liking

Scarcity

Tactics

Pretexting

Tailgating

Baiting

Phishing

Impersonation

Manipulation and Influence

Pretexting

- This is when attackers use a backstory or 'pretext' in order to gain a victim's trust
- This can be used in conjunction with other social engineering methods such as tailgating or phishing, but, it can also be used by itself to gain sensitive information

Pretexting

- Most pretexts are composed of two elements:

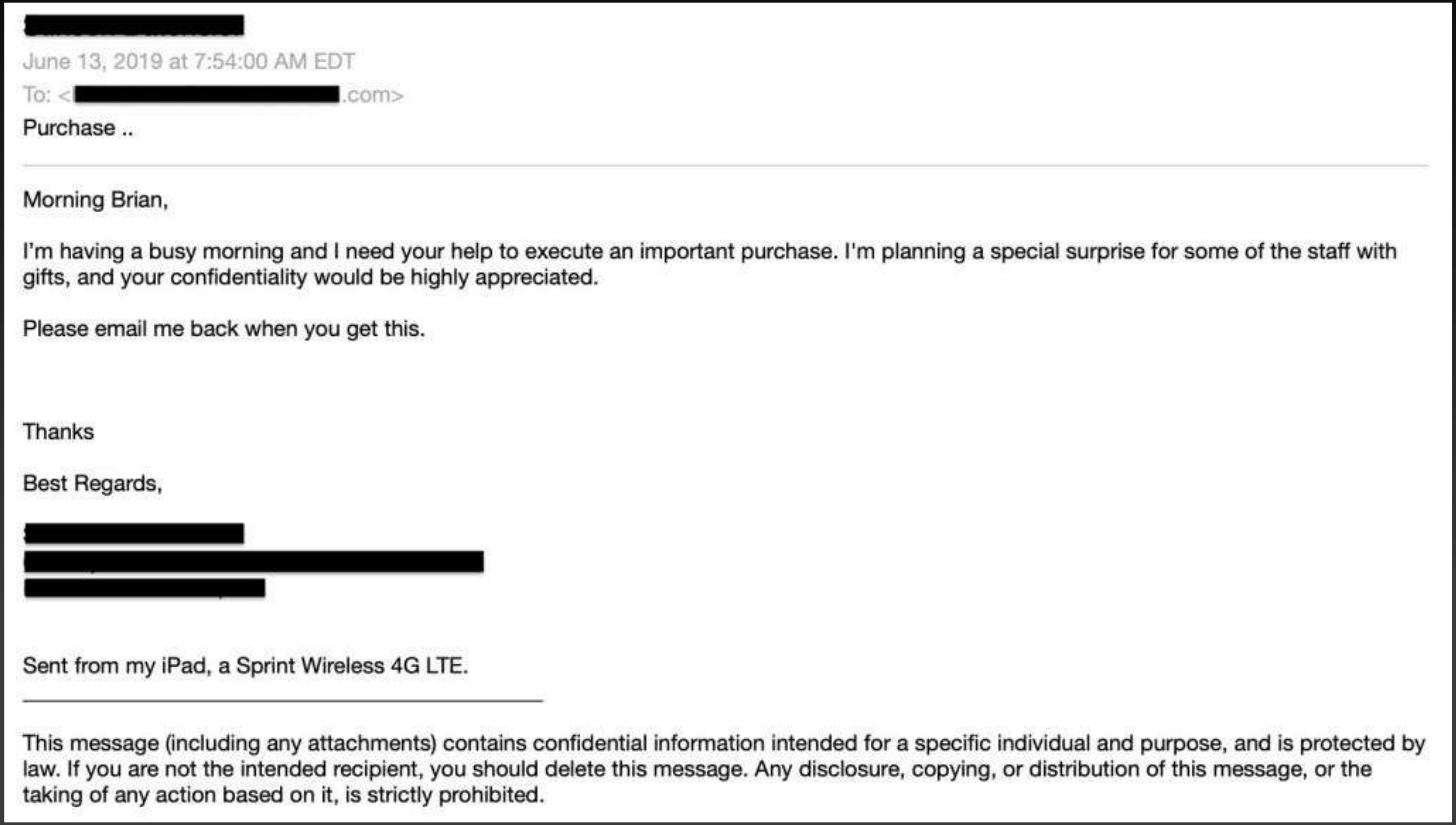
Character

This is who the attacker is posing as to seem more credible.

This is the scenario that the attacker uses in order to gain information

Situation

Pretexting - Example



[redacted]

June 13, 2019 at 7:54:00 AM EDT

To: <[redacted].com>

Purchase ..

Morning Brian,

I'm having a busy morning and I need your help to execute an important purchase. I'm planning a special surprise for some of the staff with gifts, and your confidentiality would be highly appreciated.

Please email me back when you get this.

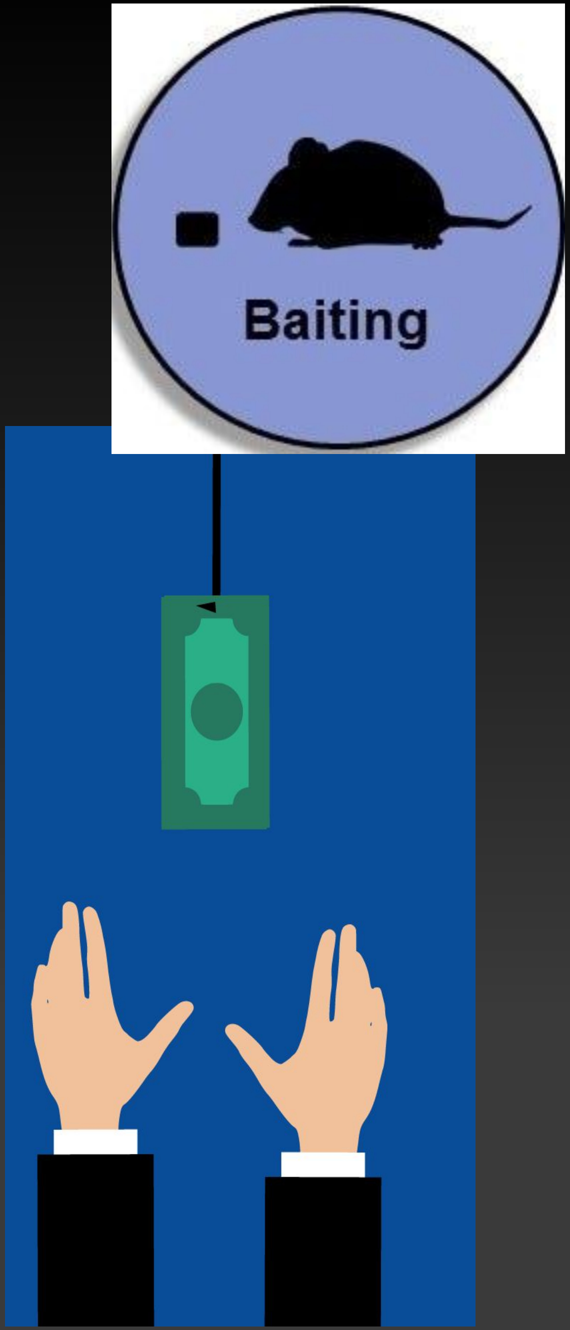
Thanks

Best Regards,

[redacted]

Sent from my iPad, a Sprint Wireless 4G LTE.

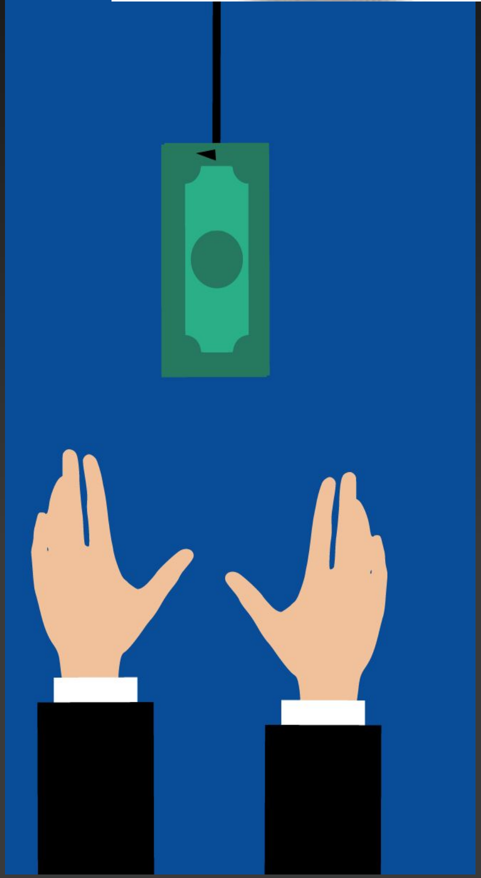
This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message. Any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.

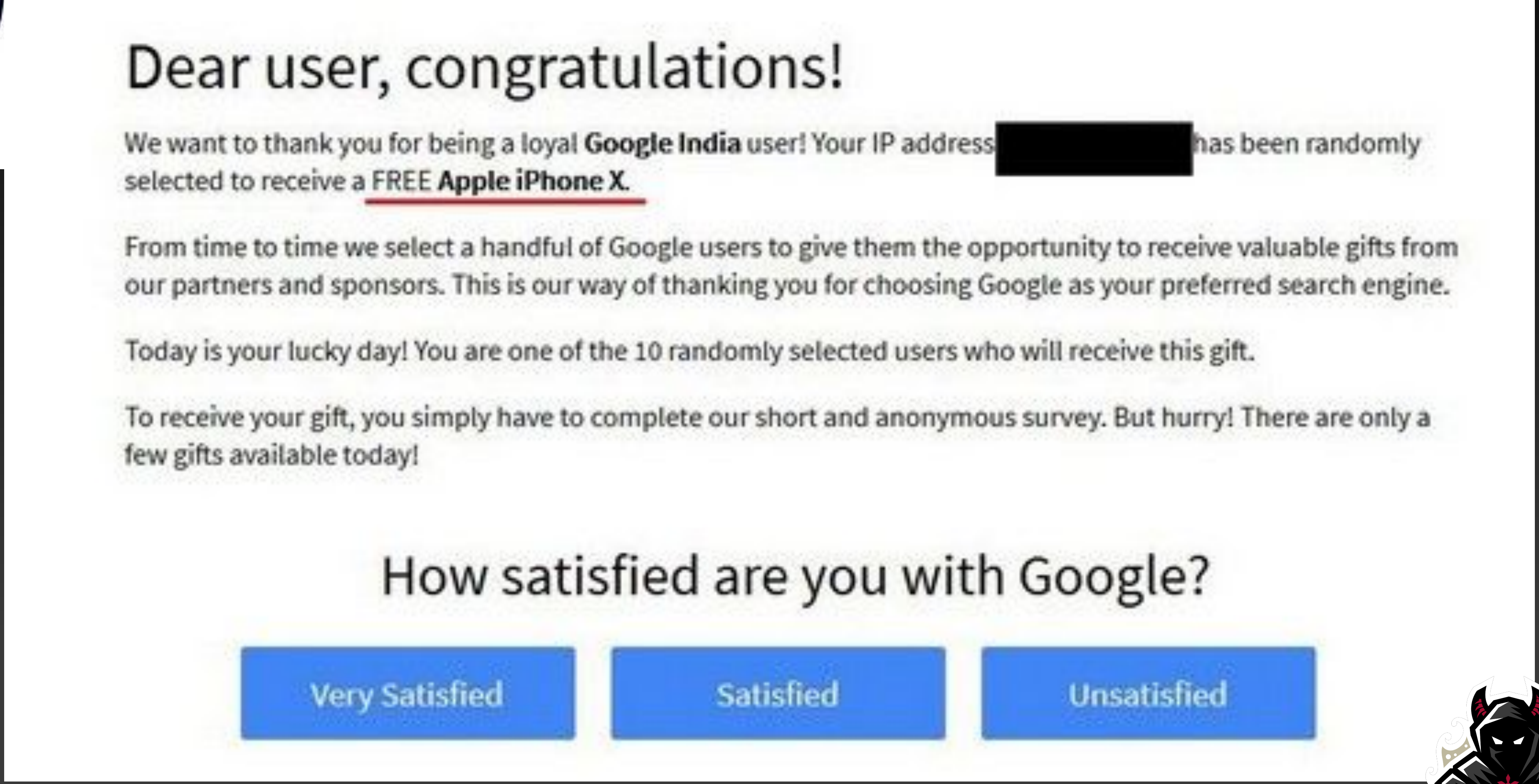


Baiting

- This is a tactic where attackers lure people in with false promises in order to gain sensitive information or to install malware onto the system
- There are multiple ways that baiting can take place
    - A 'free USB' stick found on the floor
    - An advert that offers a free Amazon voucher as you are the 1000th visitor of the website
    - A link to download to a free antivirus system

Baiting - Example





Dear user, congratulations!

We want to thank you for being a loyal **Google India** user! Your IP address [redacted] has been randomly selected to receive a FREE **Apple iPhone X**.

From time to time we select a handful of Google users to give them the opportunity to receive valuable gifts from our partners and sponsors. This is our way of thanking you for choosing Google as your preferred search engine.

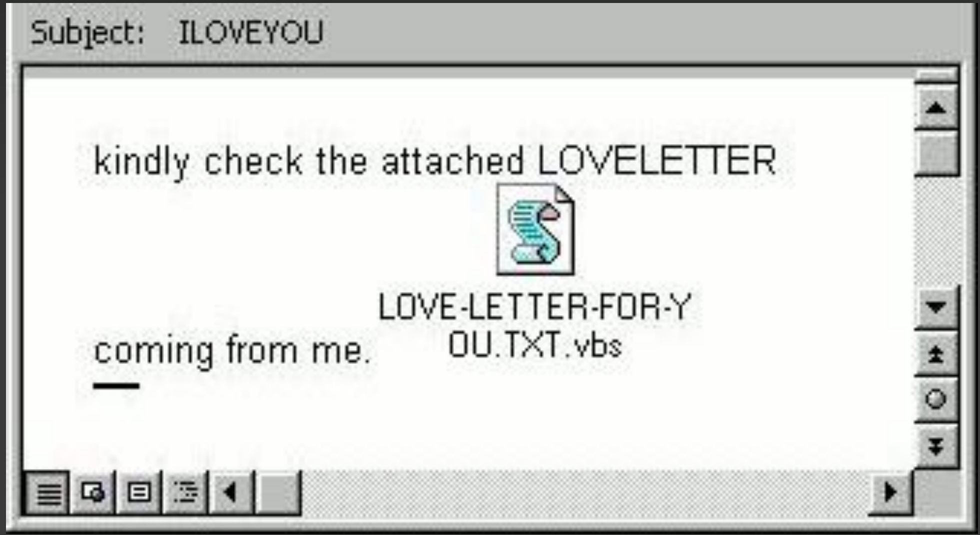
Today is your lucky day! You are one of the 10 randomly selected users who will receive this gift.

To receive your gift, you simply have to complete our short and anonymous survey. But hurry! There are only a few gifts available today!

How satisfied are you with Google?

Baiting - The Love Letter Worm

- Also referred to as ILOVEYOU
- Recipients are sent an email with ILOVEYOU as the subject and the email contained an attachment which when opened resulted in the message being sent to everyone in the recipients email address book
- On May 4, 2000 the ILOVEYOU worm spread through Microsoft Outlook
- In about 10 days, the virus had reached an estimated 45 million users and had caused $10 billion in damage

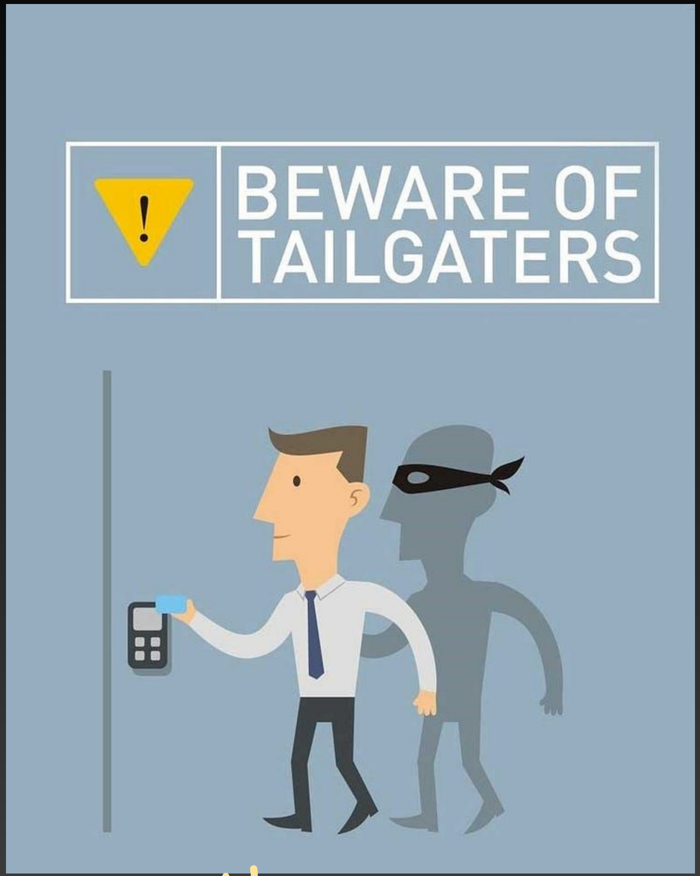


Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Tailgating

- This is when an unauthorised person follows someone into a secure area that they otherwise wouldn't have access to
- Tailgaters can:
  - Damage property
  - Install malware onto systems
  - Steal sensitive information
  - Compromise user credentials



- Piggybacking - this is similar to tailgating, however, the employee consents to providing access - the attacker poses as someone who the employee may provide access to e.g. a delivery driver or someone who's lost their badge

Impersonation

- Impersonation refers to when an attacker will pretend to be someone in order to gain access to sensitive information
- Physical Impersonation refers to when an attacker will physically disguise themselves into a different individual
  - The attacker will mimic the appearance, behaviour or credentials in order to gain access

- In order to gain access, the attacker may use disguises, forged credentials or verbal deception

Manipulation and Influence

- Manipulation and Influence are two separate things
- Manipulation refers to using guilt, shame and embarrassment to get an immediate reaction
- Influence refers to swaying the decision of another to do what you want them to, without forcing them.
- The difference between manipulation and influence is intent.
- Influence generally benefits both parties, however, manipulation usually only benefits the attacker

- Manipulation is usually a short-term solution whereas influence can have a long-lasting effect

DMU HACKERS

Phishing

- This is when attackers attempt to trick users into sharing their personal data through following a bad link or by thinking that the email is from a trusted source.
  - Phishing attacks are usually done for financial gain - such as gaining credit card details or to sell information on the dark web
  - Not all phishing emails are caught by the spam filter
  - Anyone can be a victim of phishing

Phishing

Bait

This lures in the recipient.
Is typically a deceptive email, message or communication
Looks to be from a trustworthy/ reputable source

Deception

The communication creates a sense of urgency - making the recipient act quickly
The communication looks legitimate - has logos, branding etc

Call to Action

There will be an action for the recipient to do - this could be clicking a link or transferring money/bitcoin across

Consequence

This is the aftermath of the attack - the victim has complied with their attack and their sensitive data has been stolen

Types of Phishing

Spear Phishing

These messages are highly targeted to a specific victim. The address that the message is sent from is an address that the victim is familiar with. These require knowledge about the victim as they are personalised.

Smishing

These are phishing attacks that happen over text messages. The attacker lures victims to click links or share information over text. One example is when you get fake text messages asking you to collect a parcel.

Vishing

These are phishing attacks that take place over the phone. The attacker calls victims in an attempt to gain information over the phone. A good example is when a “bank” phones a victim to gain information around their card details.

Pharming

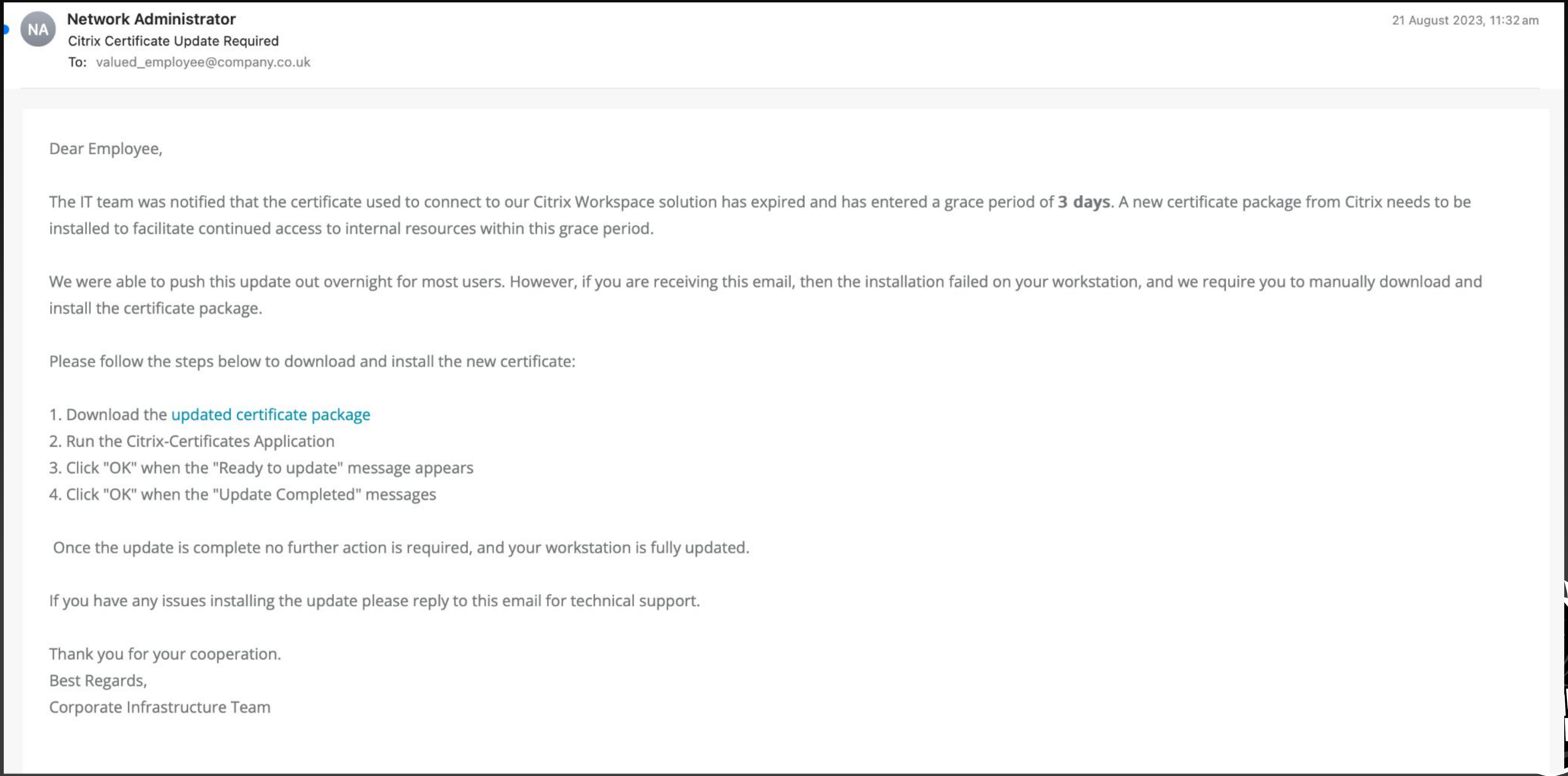
This involves the use of malicious code to direct victims to fraudulent websites in an attempt to steal their credentials and data. The victims are unaware of this as usually the website look legitimate

Whaling

This is where high-ranking executives are targeted to gain access to money or sensitive data. These have to be sophisticated as they are highly targeted

DMU HACKERS

Phishing - Example



Network Administrator
Citrix Certificate Update Required
To: valued_employee@company.co.uk

21 August 2023, 11:32 am

Dear Employee,

The IT team was notified that the certificate used to connect to our Citrix Workspace solution has expired and has entered a grace period of **3 days**. A new certificate package from Citrix needs to be installed to facilitate continued access to internal resources within this grace period.

We were able to push this update out overnight for most users. However, if you are receiving this email, then the installation failed on your workstation, and we require you to manually download and install the certificate package.

Please follow the steps below to download and install the new certificate:

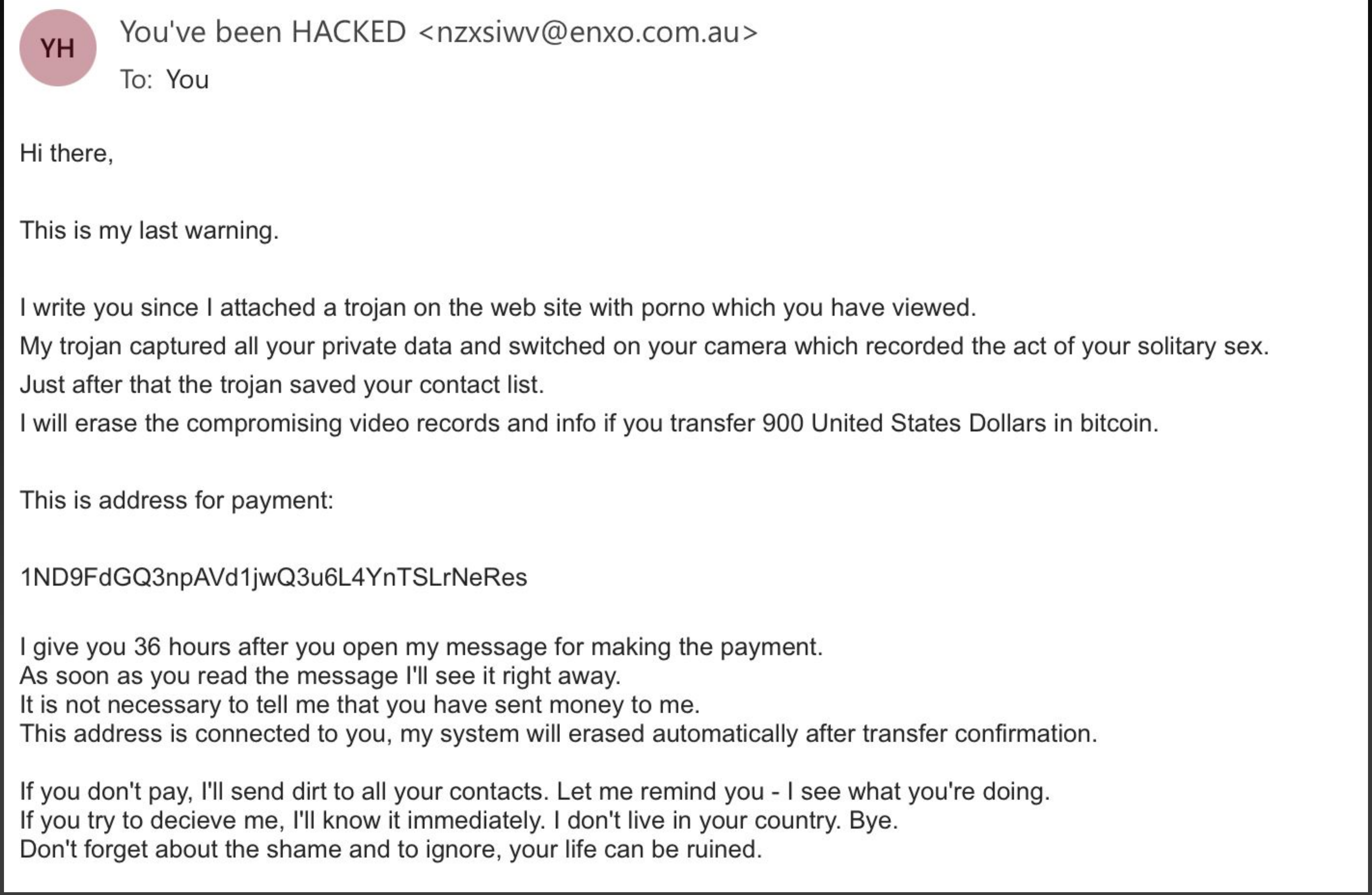
1. Download the updated certificate package
2. Run the Citrix-Certificates Application
3. Click "OK" when the "Ready to update" message appears
4. Click "OK" when the "Update Completed" messages

Once the update is complete no further action is required, and your workstation is fully updated.

If you have any issues installing the update please reply to this email for technical support.

Thank you for your cooperation.
Best Regards,
Corporate Infrastructure Team

Phishing - Example



YH

You've been HACKED <nzxsiwv@enxo.com.au>

To: You

Hi there,

This is my last warning.

I write you since I attached a trojan on the web site with porno which you have viewed.
My trojan captured all your private data and switched on your camera which recorded the act of your solitary sex.
Just after that the trojan saved your contact list.
I will erase the compromising video records and info if you transfer 900 United States Dollars in bitcoin.

This is address for payment:

1ND9FdGQ3npAVd1jwQ3u6L4YnTSLrNeRes

I give you 36 hours after you open my message for making the payment.
As soon as you read the message I'll see it right away.
It is not necessary to tell me that you have sent money to me.
This address is connected to you, my system will erased automatically after transfer confirmation.

If you don't pay, I'll send dirt to all your contacts. Let me remind you - I see what you're doing.
If you try to decieve me, I'll know it immediately. I don't live in your country. Bye.
Don't forget about the shame and to ignore, your life can be ruined.

Today's Task…

Snapped Phish-ing Line

https://tryhackme.com/room/snappedphishingline

Pub team, ASSEMBLE!
makeagif.com