SCC.141 Professionalism in Practice

Week 14: Malware, Malevolent online practices, Threat Modelling

5th February 2025
Dr Elmira Yadollahi, e.yadollahi@lancaster.ac.uk
School of Computing and Communications

*Inspired by Lecture by Dr Bran Knowles and Dr Phil Benachour previous lectures.

Learning Objectives

- **Define** different types of malware
- **Recognize** various malevolent online practices and how they exploit vulnerabilities in technologies
- **Understand** threat modelling (STRIDE, DREAD) and apply it to real-world scenarios
- **Develop** a Holistic Approach to Cybersecurity

Agenda

- **Malware Basics & Taxonomy**
- **Malevolent Online Practices:** Social Engineering, Grooming, Online Stalking, etc.)
- **Threat Modelling:** Why, how, and frameworks (STRIDE & DREAD)
- **Summary & Key Takeaways**

Lancaster University

Malware

The Weakest Link Principle

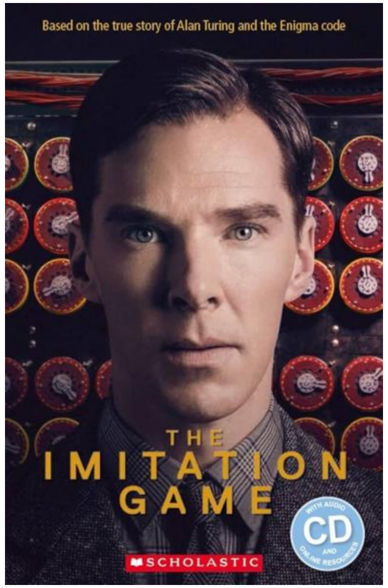
People often represent **the weakest link** in the security chain and are chronically responsible for the failure of security systems”
(Bruce Schneier, 2000, p. 149).

The Weakest Link Principle

- Exploitation of software and information systems often targets the **weakest link**:
  - **Human factors**: Social engineering, unintentional errors
  - **Technology vulnerabilities**:
    - Outdated or insecure apps
    - Operating system defects
  - **Exposed personal traits**:
    - Oversharing on social media (e.g., sensitive interests or habits)
- **Role of Designers (i.e., You!):**
  - Anticipate and mitigate potential threats
  - Build systems that prioritize **security and user awareness**

Historical Example — Enigma & “CILLY”

- **The Enigma Machine,** used at WWII, was thought unbreakable
- The Enigma’s settings offered **150,000,000,000,000,000,000** possible solutions, yet the Allies were eventually able to crack its code


Based on the true story of Alan Turing and the Enigma code
THE IMITATION GAME
WITH AUDIO CD AND ONLINE RESOURCES
SCHOLASTIC

Historical Example — Enigma & “CILLY”

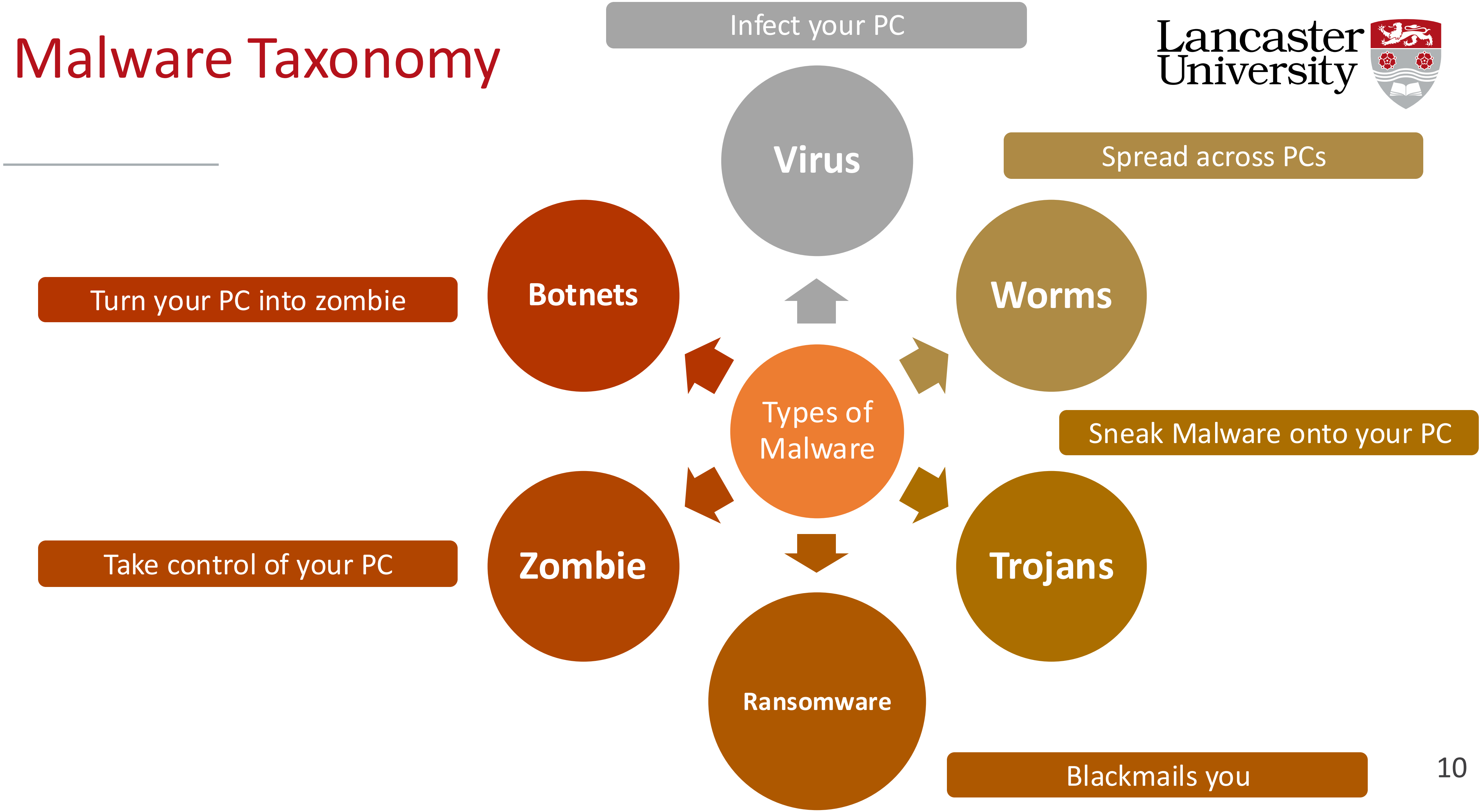
- **The Enigma Machine,** used at WWII, was thought unbreakable
- The Enigma’s settings offered **150,000,000,000,000,000,000** possible solutions, yet the Allies were eventually able to crack its code

- **Cracked** at **Bletchley Park** because of human errors
  - **CILLY** was the start of every message sent out by one particular German operator
  - This **predictable sequence of letters** was an example of regularly occurring patterns in Enigma-encrypted messages
  - The Enigma machine, when used properly, was **highly secure**
- **Lesson**: Cracking Enigma was not a machine flaw, but a human one

Defining Malware

- **What is Malware?**
  - Malware is short for **Mal**icious soft**ware**.
  - Any software designed to cause harm to computer systems, networks, or users
  - Malware can take many forms
- **What Does Malware Do?**
  - Malware is designed to **harm** and **exploit** your computer or network
  - Steal **sensitive information** like passwords and credit card numbers
  - **Disrupt** system's operations
  - Allow attackers to **gain unauthorized access** to your device

Malware Taxonomy



Types of Malware

Virus

Infect your PC

Worms

Spread across PCs

Trojans

Sneak Malware onto your PC

Ransomware

Blackmails you

Zombie

Take control of your PC

Botnets

Turn your PC into zombie

Malware Taxonomy: Virus

Virus

- **Virus** is malicious executable code attached to another executable file
  - Resident Virus (stays in memory) vs. Non-Resident Virus (Don't stay after execution)
- **How It Spreads:** Spreads through infected files
- **Impact:** Can corrupt files, slow down systems, or cause crashes
- **Prevention:** Use antivirus and avoid untrusted files
- **Example:**
  - **Conficker (2008)**
    - Virus that exploited Win32 weaknesses to create a distributed remote-controlled botnet
    - It worked by killing the tasks associated with antivirus software before it could be detected
    - 15,000,000 computers affected

Malware Taxonomy: Worm

Worms

- **Worms** are self-replicating malware that doesn’t require a host to spread
  - Compared to a virus they don’t need a host program, worms can run by themselves
- **How It Spreads:** Exploits security flaws to propagate over networks
- **Impact:** Disrupts networks and consumes bandwidth
- **Prevention:** Regular updates and firewall use
- **Example:**
  - **ILOVEYOU Worm (2000)**
    - Email attachments containing Visual Basic Script that damaged the computer by overwriting files
    - Opening the attachment sent the email to the user’s contacts

Malware Taxonomy: Trojan

Trojans

- **Trojans** are malware disguised as legitimate software to trick users to install them
  - Normally something you want!
- **How It Spreads:** Delivered through phishing or malicious downloads
- **Impact:** Steals data or provides unauthorized access
- **Prevention:** Be cautious with emails and downloads
- **Example:**
  - **Back Orifice (1998):**
    - User installs server-side program
    - 3rd party can then control/access the machine via client

Malware Taxonomy: Ransomware

Ransomware

- **Ransomware** infects computer, encrypts files or locks systems for ransom
- **How It Spreads:** Typically, via phishing emails or infected websites
- **Impact:** Data loss, financial extortion, and system downtime
- **Prevention:** Backup important files and avoid suspicious links
- **Example:**
  - WannaCry (2017)
    - Exploited a vulnerability in Windows systems
    - Encrypted files demanding Bitcoin payments
    - Spread across the globe, affecting thousands of organizations, including the NHS in the UK

Malware Taxonomy: Zombie

Zombie

Lancaster University

- **Zombie** is a compromised computer controlled by hackers to perform malicious acts
- **How It Spreads:** Zombies can be created by any malware, i.e., Trojans or worms
- **Impact:** Used in botnets for spam or Distributed Denial of Service (DDoS) attacks
- **Prevention:** Regular updates, monitor, unusual activity, and strong authentication
- **Example:**
  - **Zeus Trojan (2007)**
    - The Zeus Trojan is notorious for turning infected systems into zombies for use in a botnet
    - Typically for stealing banking credentials and launching DDoS attacks

Malware Taxonomy: Botnet

Botnets

- **Botnet** is a network of zombies controlled remotely by cybercriminals
- **How It Spreads:** Malware infiltrates devices, turning them into bots that can be used for malicious purposes
- **Impact:** Used to launch attacks like DDoS, send spam emails, or steal sensitive information
- **Prevention:** Secure IoT devices, use firewalls, and antivirus software
- **Example:**
  - **Mirai Botnet (2016)**
    - The Mirai botnet exploited unsecured IoT devices like cameras and routers
    - Turned them into bots for large-scale DDoS attacks that brought down major websites and services

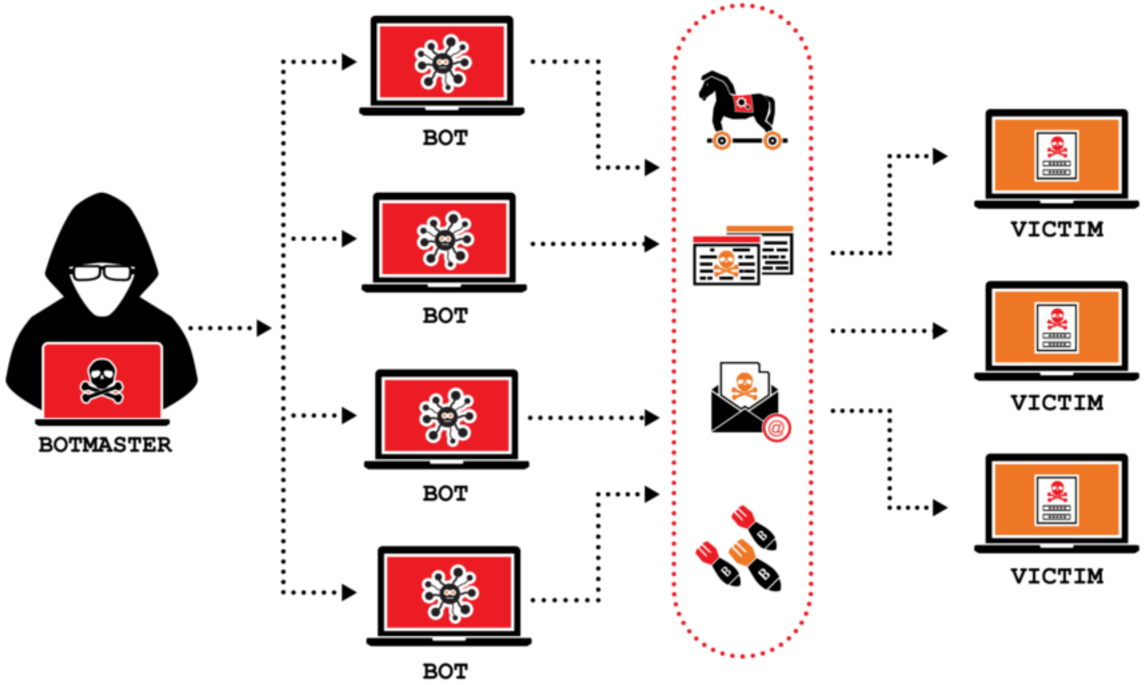
What is a DDoS Attack?

A distributed denial of service (DDoS) attack is **kind of like a traffic jam on a website**

It Involves Zombies!

What is a DDoS Attack?

A distributed denial of service (DDoS) attack is **kind of like a traffic jam on a website**



A DDoS attack is when a hacker makes a website or other service inaccessible by **flooding it with requests from many different devices**

How Malware Gains Access?

- **Phishing Emails:** Malicious attachments or links trick users into downloading malware
- **Exploiting Vulnerabilities:** Malware often takes advantage of unpatched software or system weaknesses
- **Social Engineering:** Attackers manipulate victims into revealing sensitive information or executing malicious code
- **Malicious Websites/Ads:** Malware is delivered through compromised or fake websites and ads
- **Infected Software/Downloads:** Malware can hide in seemingly legitimate software or files

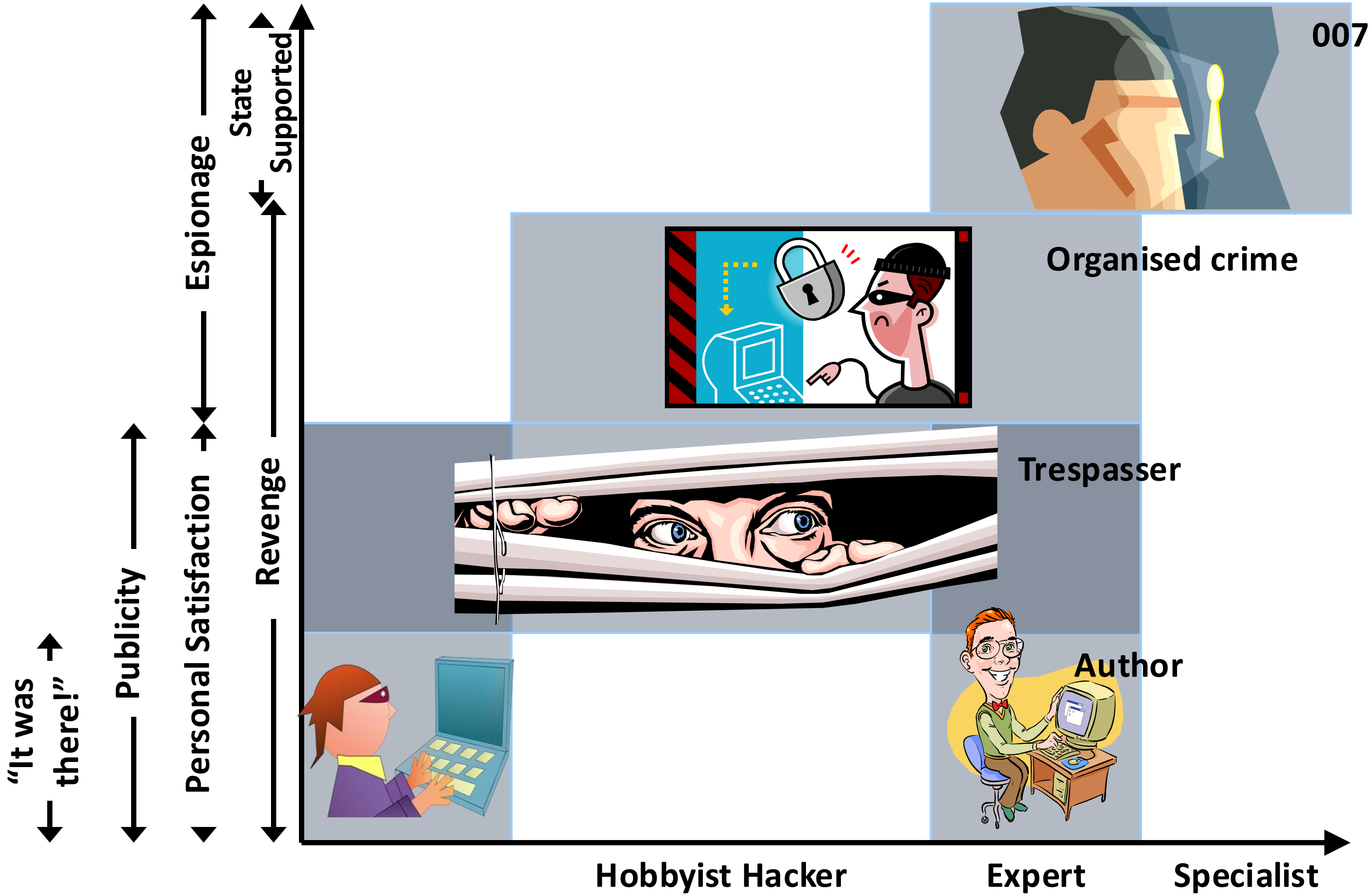
What Are the Effects of Malware?

- **Data Theft:** Personal, financial, or business data is stolen for malicious use
- **System Damage:** Malware can corrupt or delete files, slow down or crash systems
- **Loss of Privacy:** Sensitive information such as passwords or browsing history may be exposed
- **Financial Loss:** Ransomware and data breaches can lead to direct financial damage
- **Performance Issues:** Malware can reduce system speed or disrupt normal operation
- **Reputation Damage:** Organizations or individuals may suffer from compromised trust and credibility

Who Are Malware Practitioners?

- **Cybercriminals:** Individuals or groups who create and distribute malware for financial gain
- **Hacktivists:** People or organizations who use malware as a tool for political or social causes
- **State-Sponsored Actors:** Governments or military organizations that use malware for espionage, sabotage, or warfare
- **Script Kiddies:** Less skilled attackers who use pre-made malware for fun or to gain attention
- **Cybersecurity Researchers:** Ethical hackers who analyze malware to develop protections or solutions (often the counterforce to malicious actors)

Who: Malware Practitioners



Malevolent Online Practices

Malevolent Online Practices

- Creation and use of malware is **NOT** the only malevolent practice on the Web…
- Rise of social networks & digital communication → **New malicious practices**
- Often target vulnerable groups:
  - Elderly people
  - Single men and women
  - Children
- **You** need to be able to spot these practices

Malevolence I: Phishing

- **Phishing**: Spam emails containing a **convincing hyperlink**
  - Looks like it’s from a trusted source
  - Actual address may be foreign or suspicious
  - Victims tricked into entering personal info
  - Clicking confirms your email is active → **more spam!**
- **Examples:** Banks, tax agencies, social media

- **Compare** with **spear-phishing**

Malevolence I: Phishing

- **Phishing**: Spam emails containing a **convincing hyperlink**
  - Looks like it's from a trusted source
  - Actual address may be foreign or suspicious
  - Victims tricked into entering personal info
  - Clicking confirms your email is active → **more spam!**
- **Examples:** Banks, tax agencies, social media
- **Compare** with **spear-phishing**
  - A more **targeted and personalized** form of phishing where attackers tailor their fraudulent messages to a specific individual or organization

Malevolence I: Phishing

- **Phishing**: Spam emails containing a **convincing hyperlink**
    - Looks like it's from a trusted source
    - Actual address may be foreign or suspicious
    - Victims tricked into entering personal info
    - Clicking confirms your email is active → **more spam!**
- **Examples:** Banks, tax agencies, social media

- **Compare** with **spear-phishing**
    - A more **targeted and personalized** form of phishing where attackers tailor their fraudulent messages to a specific individual or organization

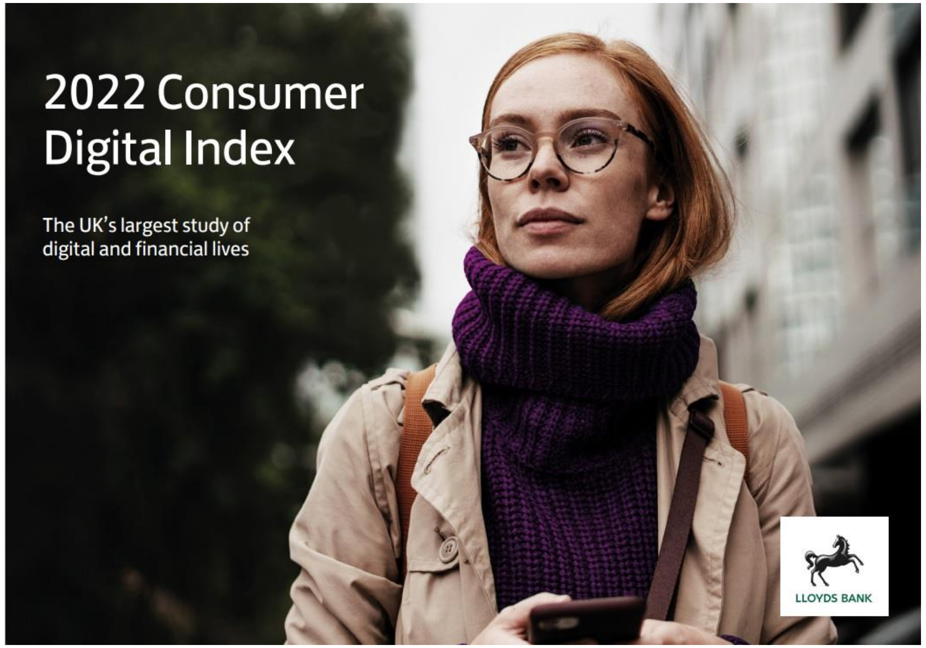
Evolving risks to (formerly) excluded

- Many older adults going online for the first time during Covid
- **660%** increase in phishing attacks aimed at older adults

WHITEPAPER

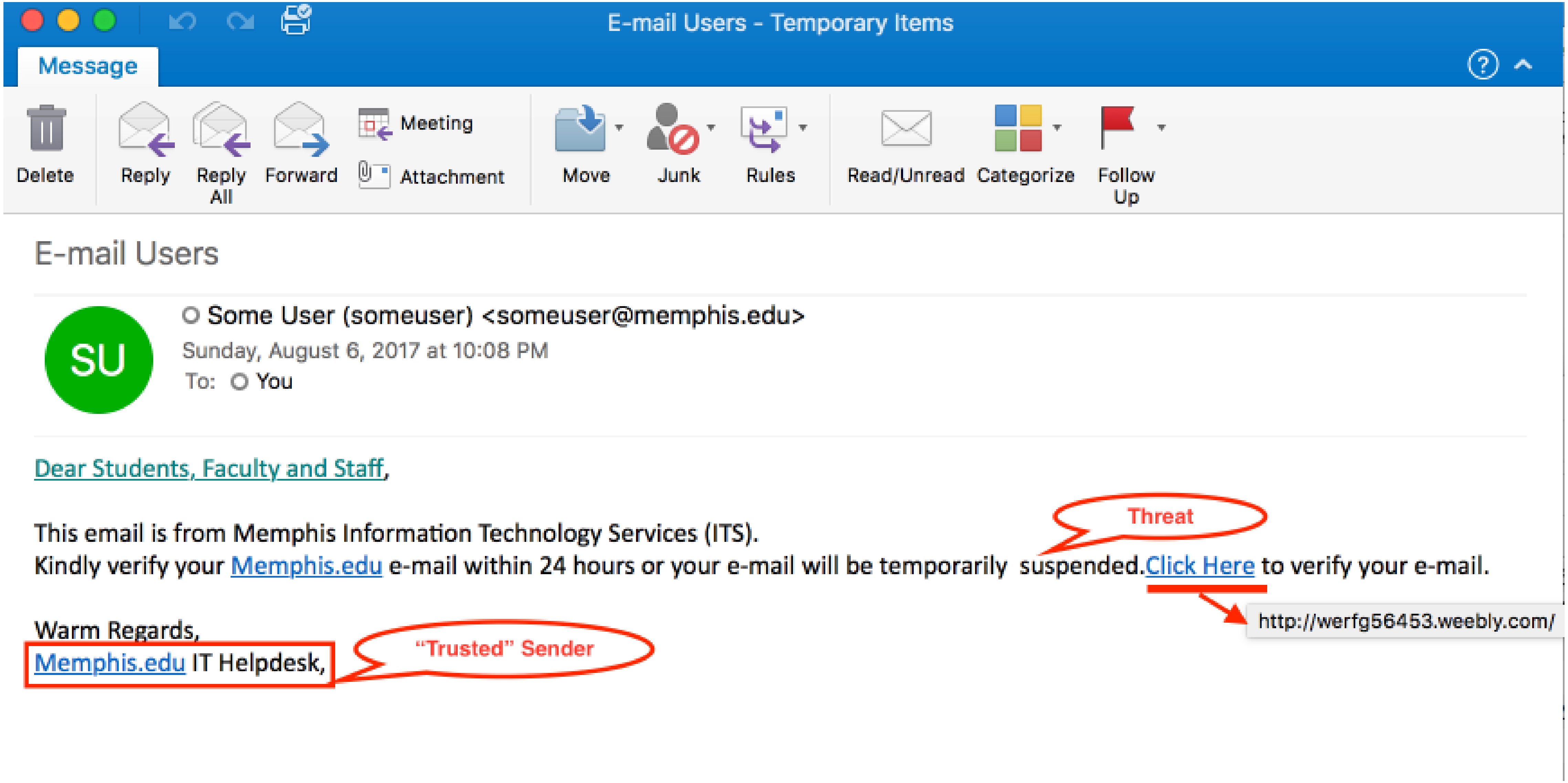
THE GLOBAL YEAR IN BREACH 2021:

What Happened in 2020, Why It Happened and What To Do Next



2022 Consumer Digital Index

The UK's largest study of digital and financial lives



E-mail Users

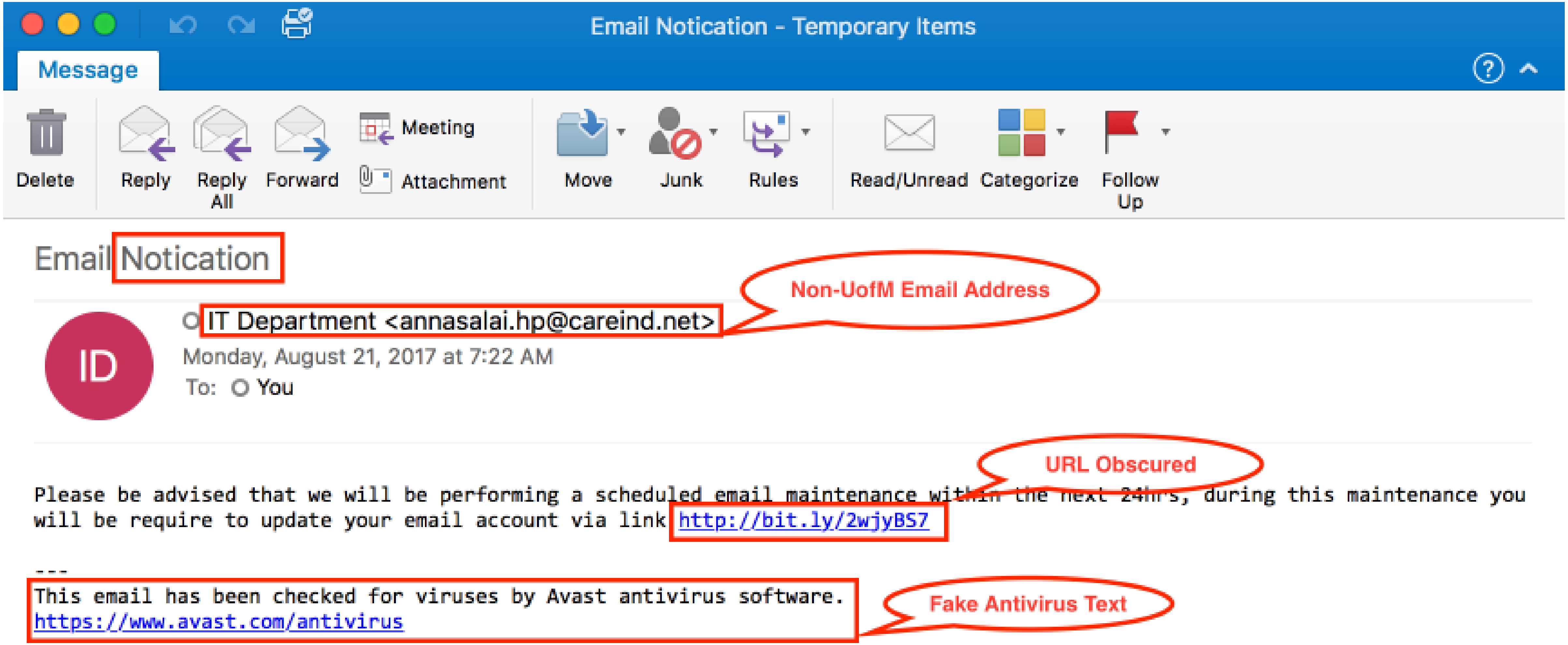
○ Some User (someuser) <someuser@memphis.edu>
Sunday, August 6, 2017 at 10:08 PM
To: ○ You

Dear Students, Faculty and Staff,

This email is from Memphis Information Technology Services (ITS).
Kindly verify your Memphis.edu e-mail within 24 hours or your e-mail will be temporarily suspended.Click Here to verify your e-mail.

Warm Regards,
Memphis.edu IT Helpdesk,

https://www.memphis.edu/its/security/phishing-examples.php



Email Notication

IT Department <annasalai.hp@careind.net>

Monday, August 21, 2017 at 7:22 AM

To: You

Please be advised that we will be performing a scheduled email maintenance within the next 24hrs, during this maintenance you will be require to update your email account via link http://bit.ly/2wjyBS7

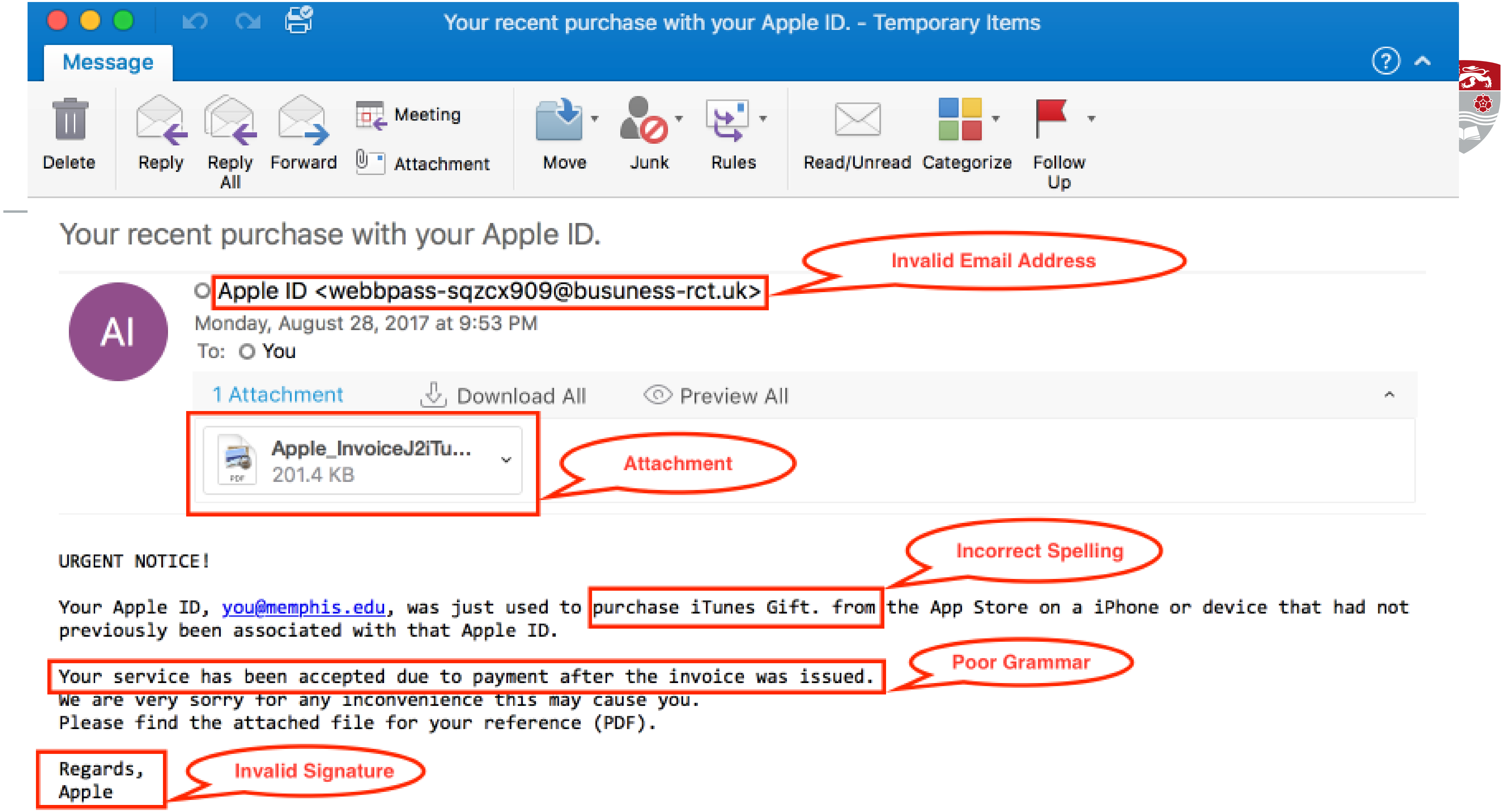
This email has been checked for viruses by Avast antivirus software.
https://www.avast.com/antivirus

Non-UofM Email Address

URL Obscured

Fake Antivirus Text

https://www.memphis.edu/its/security/phishing-examples.php



Your recent purchase with your Apple ID.

Apple ID <webbpass-sqzcx909@busuness-rct.uk>

Invalid Email Address

Monday, August 28, 2017 at 9:53 PM

To: You

1 Attachment Download All Preview All

Apple_InvoiceJ2iTu...
201.4 KB

Attachment

URGENT NOTICE!

Your Apple ID, you@memphis.edu, was just used to purchase iTunes Gift. from the App Store on a iPhone or device that had not previously been associated with that Apple ID.

Incorrect Spelling

Your service has been accepted due to payment after the invoice was issued.
We are very sorry for any inconvenience this may cause you.
Please find the attached file for your reference (PDF).

Poor Grammar

Regards,
Apple

Invalid Signature

https://www.memphis.edu/its/security/phishing-examples.php

Malevolence II: Social Engineering

- Social engineering is often described as **"hacking without code"**
- Based on the **principle of trust**
- The perpetrator collects data through:
  - **Dumpster diving** (that's why you should always shred documents!)
  - Monitoring social media e.g., Facebook and Twitter
  - **Shoulder surfing** (peeking at screen in public)
- The perpetrator convinces the victim to trust them, ask for money/details:
  - Via a dating site
    - Serious Organized Crime Agency reported 200k victims in the UK up to 2011
- Contact methods: email, telephone, social networking sites

Malevolence III: Grooming

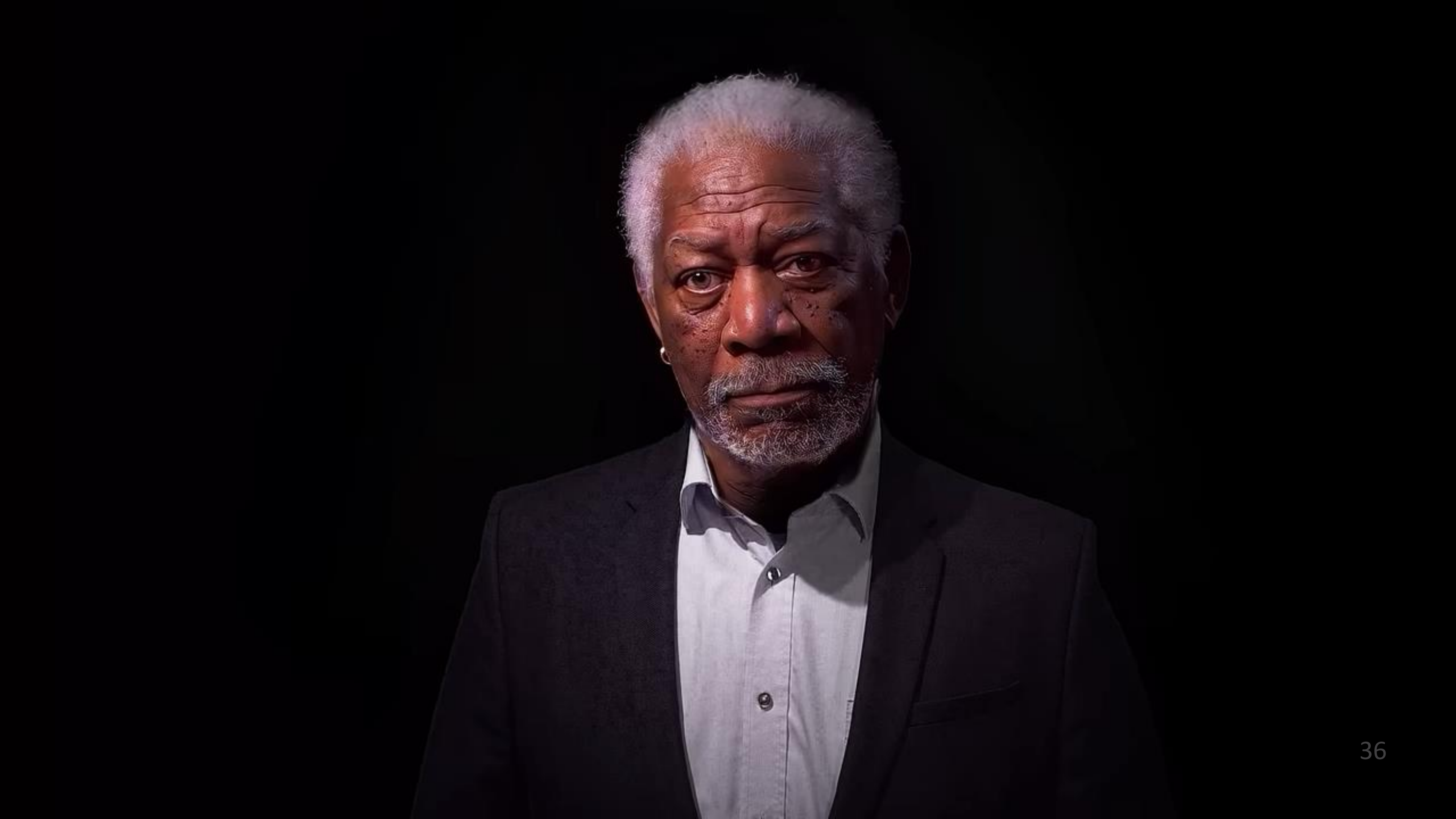
- **Gaining trust** of a victim by being nice over time
  - Often a **long** process of building rapport
- Once trust has been gained and established:
  - Get the victim to **reveal information** about themselves
    - i.e. key personal data for online banking
  - Involve them in a crime **unknowingly**
    - Handling stolen goods, provision of alibis
- Not just restricted to paedophiles:
  - Romance scams con single adults out of money

Malevolence IV: Online Stalking

- **Stalking:** obsessively following or watching a person without their knowledge
  - Often **“lateral”** (covert) surveillance
  - Increase due to social networks:
    - Checking a former partner’s statuses or updates
- **Lateral surveillance:** viewing someone’s online presence without their knowledge
  - Employers do background checks online
- **Doxing:** publishing private data (addresses, phone numbers) with malicious intent

Malevolence V: Deepfakes & Synthetic Media

- **Deepfakes:** AI-generated images, videos, or audio that appear real
  - Technology uses machine learning to mimic faces, voices, or actions
- **Applications in Cybercrime:**
  - Impersonating executives for fraud (e.g., fake calls or emails)
  - Creating fake evidence for blackmail or manipulation
  - Spreading misinformation or fake political speeches
- **Broader Implications:**
  - Challenges in verifying authentic media
  - Potential for eroding trust in digital content



Malevolence VI: Misinformation & Propaganda

- **Misinformation:** Sharing false or misleading information unintentionally
- **Disinformation:** Deliberate spread of false information to manipulate or deceive
- **Techniques:**
  - **Fake news**, doctored images, AI-generated content
  - **Bots** and **fake accounts** amplifying narratives
  - Deepfakes used to **fabricate speeches** or events
- **Impacts:**
  - Erodes trust in media and institutions
  - Polarizes society and amplifies echo chambers
  - Influences political outcomes and public opinion

Lancaster University

Threat Modelling

Threat Modelling

- **What is threat modelling?**
  - A technique within the security lifecycle to analyze a system’s security & privacy concerns

- **Why threat model?**
  - Recognize **potential failures** or attacks
  - Identify design & implementation **flaws** early
  - Inform **decisions** throughout development, testing, & deployment

Assets, Threats and Risks

- **5 Key phases of Threat Modelling**

- Asset Identification
- Threat Analysis
- Vulnerability Analysis
- Risk Assessment
- Risk Communication

Assets, Threats and Risks

- **5 Key phases of threat modelling**

Asset Identification	Determine what you’re trying to protect
Threat Analysis	Identify potential attacks or events that could compromise these assets
Vulnerability Analysis	Pinpoint the weaknesses in the setup–both technical and organizational
Risk Assessment	Evaluate the likelihood and impact of each threat
Risk Communication	Share the findings with stakeholders (developers, management, end-users)

Assets, Threats and Risks

- **5 Key phases of threat modelling**

- Asset Identification
- Threat Analysis
- Vulnerability Analysis
- Risk Assessment
- Risk Communication

- **These phases identify:**

- Which assets need protection
- Relevant threats & vulnerabilities
- Risk level for each threat
- Mitigation & contingency priorities

What is a Threat Agent?

- **Natural threats and/or accidents**
  - Non-intentional threat agents (e.g., floods, fires, user mistakes)
- **Malicious agents**
  - Intentional actions, the ones everyone thinks of
  - **Characteristics**
    - Motivation
    - Capability
    - Access
    - Amplifiers
    - Inhibitors

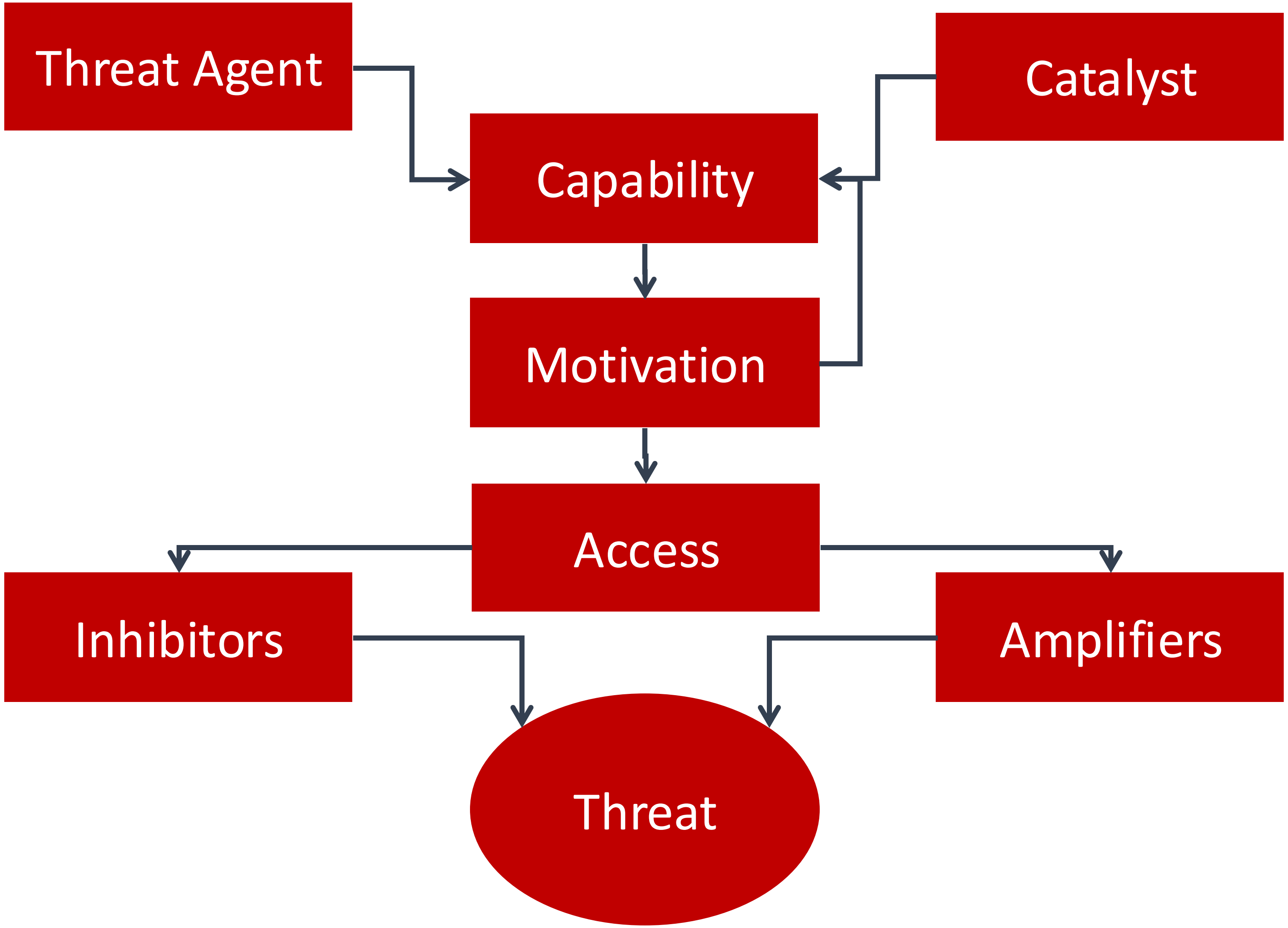
Natural and Accidental Threats

- **Natural**
  - Well-studied (insurance data, actuarial tables)
  - Relatively predictable in terms of frequency so organizations can plan accordingly
- **Accidental**
  - Come from human error with no malicious intent
    - lost or stolen devices, misconfigurations, or employees clicking on phishing links
  - Hard to track
  - Implement **awareness training**, **strict policies** around data handling, and proper **incident reporting**

Malicious Agents

- **Definition:** An agent can be an individual or group that implements a threat
  - Influenced by amplifiers(motivators, resources, alliances) or inhibitors (legal risk, limited access, fear of exposure)
- **Characteristics:**
  - **Motivation:** Why do they act?
  - **Capability:** Skills & resources
  - **Catalyst:** What triggered the action?
  - **Inhibitors:** What might deter them?
  - **Amplifiers:** What might push them forward?
- **Success Factors:**
  - An **exploitable vulnerability** and a **system worth attacking**

Sequence of Factors



Threat Modeling Frameworks

- **STRIDE** and **DREAD** threat models are frameworks used in threat modeling
- They are systematic processes to identify and assess security risks in a system

- **STRIDE** is a mnemonic that categorizes potential threats based on the types of attacks they represent
  - Each letter corresponds to a specific category of threat:
- **DREAD** is a risk assessment model that evaluates threats based on five criteria
  - It’s a scoring system designed to prioritize and quantify risks

STRIDE Threat Model

	Threat Type	Description	Security Control
S	Spoofing	Impersonating a user, device, or system to gain unauthorized access	Authentication
T	Tampering	Unauthorized modification of data during transit or at rest	Integrity
R	Repudiation	Denying performing an action, often due to a lack of proper logging or auditing	Non-repudiation
I	Information Disclosure	Unauthorized access to sensitive data	Confidentiality
D	Denial of Service	Disrupting service availability by overwhelming the system or exploiting weaknesses	Availability
E	Elevation of Privilege	Gaining unauthorized, higher-level access to the system	Authorization

DREAD Threat Model

	Threat Type	Description	Score between 1 to 10
D	Damage Potential	How bad would the impact be if the threat is realized?	Nothing ------ system compromised
R	Reproducibility	How easy is it for an attacker to replicate the threat?	Hard ------ Easy, no skill required
E	Exploitability	How easy is it for an attacker to launch the attack?	Bespoke tool ------ commonly available
A	Affected Users	How many users or systems would be impacted?	None ------ All
D	Discoverability	How likely is it that the vulnerability will be found by attackers?	Hard ------ Easy

Key Takeaways

- Understanding **malware types** is essential for effective prevention and response
- Cybercriminals exploit **trust** and **human behaviour** via phishing, grooming, social engineering, and stalking
- **Threat Modelling** is a proactive method to building secure systems
- **Core Message**
  - Cybersecurity is a balance of addressing **technical vulnerabilities** (e.g., malware, system weaknesses) and **human factors** (e.g., phishing, social engineering)

Future Outlook

- **Questions?**

- **Looking Ahead:** Next week—Digital Exclusion

Lancaster University

Thank you for attending, any questions?