**Cyber Awareness – Technical Information (For Review)**

Below is the technical information that is included in the training. Each piece is revealed as a ‘case update’ once the user has completed the relevant tasks.

Each time the case is updated they will be shown the following screens. The first page will recap on the story, characters involved, and the evidence found.

A screenshot of a book

Description automatically generated

The second page will then delve into either technical information about one of the methods used by the cybercriminals in this part of the story, or information about a real-life case where this method was used.

**A screenshot of a book

Description automatically generated**

|  |
| --- |
| #1 THE MYSTERY CALLER |
| *I’ve been hired by James to investigate a potential hack at the WattNext office. Edith received an email from EcoCorp and was initially suspicious because it mentioned Project Gaia, their top-secret green energy technology. She spotted several more indicators that convinced her to report it as a phishing email.* |
| **Summary Information: Spear Phishing** |
| Edith was targeted by a “Spear Phishing” email. Unlike regular phishing, the attacker knows something about their target. Well-crafted phishing emails pretend to come from someone the victim knows or works with. |
| **Remember:**   * Don’t click on any link unless you are confident of its origin and/or destination. * Is there a pressure to take action? They are often written with a sense of urgency or impending time constraint. * Report the email as phishing, even if you’re not 100% sure it is. It's better to be safe than sorry. |

|  |
| --- |
| #2 BAITING THE TRAP |
| *The hacker must have used Mohamed’s ID card to enter the building. Once inside they placed bait in the office, specifically, a poster containing a malicious QR code on the noticeboard.*  *Looks like Joan may have fallen for the QR poster scam and could even end up spreading the scam to her friends. The hacker may have targeted her through social media and kept an eye on what she was posting.* |
| **Summary Information: QR Code Scams** |
| QR code scams are a relatively new form of phishing attack, where scammers create malicious QR codes that redirect victims to bogus websites designed to steal personal information.  In this case, Joan has been targeted through her social media posts. The hacker, exploiting her posts, was able to engineer the perfect scam by designing a poster with a QR code promoting a too-good-to-miss pet food offer. |
| **Remember:**   * QR codes are extremely easy to create and use, which makes them attractive to criminals. * Be mindful of the information you share on social media. Criminals can use this to craft targeted scams or even guess your security questions. * Whether it's a QR code, a link in an email, or a social media post, always exercise caution before clicking. If something seems too good to be true, it probably is. |
| #3 THE MESSY DESK |
| *It seems that our hacker didn't just rely on digital trickery. Gaining physical access to the office allowed them to exploit a glaring vulnerability: a messy and unsecured workstation.*  *Edmond's careless habits provided a treasure trove of information for the hacker, including contact details, his password, and even the 'Project Gaia' folder. This information was likely used to craft the targeted phishing email sent to Edith.* |
| **Summary Information: Workplace Security** |
| This highlights a critical point: cybersecurity isn't just about firewalls and antivirus software. It's about vigilance, awareness, and good old-fashioned tidiness!  A secure office environment is crucial for protecting sensitive information and preventing cyberattacks. Even in our increasingly digital world, physical security measures and responsible workplace habits play a vital role in our overall cybersecurity strategy. |
| **Remember:**   * Lock your terminal when not in use – even if just popping to the coffee machine. * Clear desks of all information before leaving. * If you are struggling to remember passwords, use a password manager like [KeePass](https://keepass.info/download.html). Failing that, write them down but keep them in a safe place! |

|  |
| --- |
| #4 THE JOB APPLICATION |
| ***Positive Outcome:***  *Lewis's instincts were right on the mark. That job application, while seemingly legitimate, was a wolf in sheep's clothing – a carefully crafted phishing attempt designed to slip through the cracks.*  *What tipped Lewis off? It wasn't just the slightly odd wording; it was the fact that it completely bypassed standard recruitment procedures. Arriving directly in his personal inbox, rather than through the usual channels, was a major red flag.*  *This case underscores a crucial point: strong cybersecurity relies on established processes and a healthy dose of scepticism. When something deviates from the norm, even something as mundane as a job application, it's crucial to question it.*  ***Negative Outcome:***  *Oops. Seems I misjudged that one. Lewis's instincts were right on the mark – that job application was indeed a cleverly disguised attempt to infiltrate WattNext's systems. Unfortunately, my advice to investigate further backfired. Opening that attachment unleashed a torrent of malware, potentially compromising sensitive data and disrupting operations.*  *This serves as a harsh reminder that even with the best intentions, curiosity can lead to unintended consequences. It also reinforces the importance of adhering to established procedures and reporting anything suspicious, even if it seems harmless on the surface. Sometimes, the best offense is a good defence.* |
| **Summary Information: Real-World Example** |
| Job applications are a common target for hackers, both for those recruiting, and for those applying for jobs.  A real-life case of this began what is known as the Bangladeshi Bank Heist, thought to have been committed by the infamous North-Korean backed hackers, the Lazarus Group. |
| **What Happened:**   * Hackers targeted bank employees on LinkedIn and Facebook who were likely involved in recruiting. * The phishing email contained a seemingly harmless document, when opened, unleashed malware that granted the hackers access to the bank's internal network. * A simple typo in one of the fraudulent transfer requests, misspelling the name of a Sri Lankan non-profit organisation, raised red flags and ultimately prevented the theft of an additional $850 million. |

|  |
| --- |
| #5 THE WHATSAPP REQUEST |
| ***Negative Outcome:***  *It seems our hacker had one more trick up their sleeve. Exploiting the accessibility of messaging apps and the deceptive power of voice cloning technology, they pulled of their main objective.*  *The forged voice note, convincingly mimicking James's voice, instructed Florence to transfer funds to a fraudulent account. Unfortunately, a lack of scrutiny and a failure to verify the request led to a costly mistake. This incident serves as a stark reminder that even the most seemingly authentic communication can be manipulated for malicious purposes.*  ***Positive Outcome:***  *The hacker's final gambit involved a daring combination of social engineering and cutting-edge technology. A voice-cloned message, seemingly from James, instructed Florence to transfer funds to a new account. However, a keen eye for detail and a commitment to security protocols saved the day.*  *By questioning the unusual request and insisting on verification, the scam was exposed, preventing a significant financial loss. This close call reinforces the importance of remaining vigilant and employing a zero-trust approach, even when dealing with familiar platforms and trusted individuals.* |
| **Summary Information: Messaging Apps** |
| The attempted scam targeting Florence highlights the growing threat of cybercriminals exploiting popular messaging apps like WhatsApp.  These platforms, designed for quick and easy communication, can also be used to spread misinformation, deliver malware, and phish for sensitive data.  What makes this case particularly alarming is the use of voice cloning technology. With just a small audio sample, hackers can now create incredibly convincing replicas of anyone's voice. This allows them to impersonate trusted individuals and manipulate their victims into divulging confidential information or authorising fraudulent transactions. |
| **Remember:**   * Be wary of unexpected requests, even if they appear to come from someone you know. * Look out for unusual language, urgent demands, unknown links or attachments to download. * If you receive a suspicious message, verify the sender's identity through another channel before taking any action. |