Institiúid Teicneolaíochta Leitir Ceanainn

Letterkenny Institute of Technology

Logo

Description automatically generated

Cybersecurity

Assignment 1

Date due: 14/04/2022

Lecturer: Saim Ghafoor

Contents

[Part 1: Security report 3](#_Toc100872927)

[Purpose 3](#_Toc100872928)

[Task 1 3](#_Toc100872929)

[Task 2 10](#_Toc100872930)

[Task 3 12](#_Toc100872931)

[Part 2: Penetration testing 13](#_Toc100872932)

[Task 1 13](#_Toc100872933)

[Part 3: Traffic Analysis 14](#_Toc100872934)

[Task 1 14](#_Toc100872935)

[Bibliography 15](#_Toc100872936)

# Part 1: Security report

## Purpose

The objective of this report is to expand on the Bank of Ireland’s current security awareness through detailing the companies’ most important data assets that will require protection, the most recent cybersecurity threats that are relevant to financial institutions and addressing any concerns with attackers accessing private parts of the company as well as any vulnerabilities that may stem from internet presence. Suggestions of security measures will also be included within this document.

## Task 1

1.1 Business overview

Bank of Ireland is one of Ireland’s largest and oldest bank institutions. From a business perspective the institution is primarily involved in banking services, expanding into five divisions, four of which relate to trading and one dedicated to customer service (Bank of Ireland 2022a). It is important to give a general overview of these divisions as each give insight into the type of data assets the institution may have.

The divisions are as follows:

1. Retail Ireland: A lender focusing on businesses struggling with arduous trading circumstances. This division offers an array of financial services including the management of a business’ finances.
2. Wealth and Insurance: Offers several types of insurance such as life and pension to customers.
3. Retail UK: Runs a banking institution in Northern Ireland and dispenses products under its brand.
4. Corporate and Treasury: Comprises of Bank of Ireland’s banking and financial markets, acquisition finance and transaction property lending business within Ireland as well as internationally in several countries.
5. Group Centre: Involves Bank of Ireland’s main control functions to include governance establishment and overseeing policies.

As a banking institution, Bank of Ireland works with very sensitive data assets that must be kept secure and protected. It is important to highlight which of these assets need to be given the most priority for protection.

1.3 Data Asset/Crown Jewel Identification

Crown jewel is a term for a companies most important data assets where they must be kept secured and protected in order for the company to continue running. For the sake of readability, the identified data assets will be assorted into a numbered list.

1. User data: Bank of Ireland works with extremely sensitive and personal user data. With the prevalence of GDPR it is imperative that this asset is kept protected. Examples of user data that is collected by this company include (Bank of Ireland 2021):
   1. PPS number, contact details, name and date of birth even including social media handles.
   2. Bank account details such as IBAN, transactions and credit history.
   3. Marital status or any form of connection to another person in the context of finance.
   4. Medical records in the events of life insurance claims
   5. Biometric data
2. Online banking: As a banking institution, the public website for bank of Ireland also includes online banking. In a digitalised era, it is vital for the company’s continuity to ensure that this is always available to their customers, especially as online banking is assured to be available 24 hours for every day of the year (Bank of Ireland 2022b).
3. Mortgage rate listing: It is vital that the mortgage rates are accurate and not manipulated.

1.4 Malware Threat Websites

It is important to keep up to date with the latest malware threats. Given that the world of cybersecurity and computing in general is fast changing, websites that are frequently releasing accurate information is essential. Four websites that are useful for getting details of these threats are:

1. The hacker news: A website that focuses on cybersecurity related news. Being very popular worldwide as well as widely recognised, it is a trusted site for those working within the computing industry to use (The Hacker News 2022).
2. Dark reading: A long-running website widely used by cybersecurity professionals to learn of the latest threats. Its community comprises of cybersecurity researches, specialists and more. The website has a useful search feature for specific articles, in this case searching malware provides us with the latest news (Jackson Higgins *et al.* 2022).

Graphical user interface, text, application, website

Description automatically generated

*Figure 1. Image of malware search results on the DARKReading website*

1. IT Security Guru: Features the latest IT security related news on a daily basis in a summarised, easy to read format (IT Security Guru 2018).

Graphical user interface, website

Description automatically generated

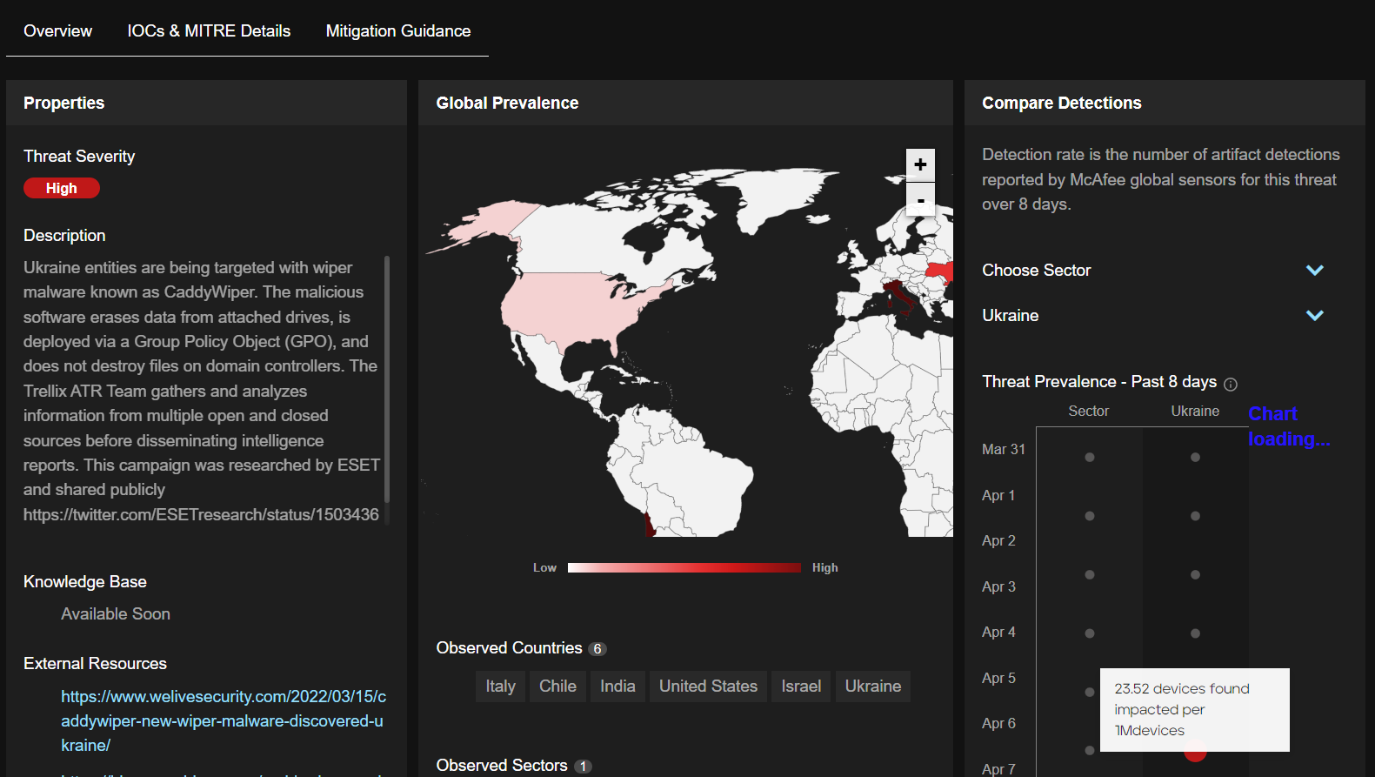
*Figure 2. Image of malware search results on the IT Security Guru website*

1. Trellix: Formerly FireEye & McAfee Enterprise is a company that focuses on developing technology that can learn and evolve to defend against threats (Sheridan 2022). The Trellix website features an updated report of the latest threats within cybersecurity, including malware and labels the severity of the threat from low to high. These threats are reported in great detail by the Trellix threat research team (Trellix 2022).

A screenshot of a computer

Description automatically generated with medium confidence

*Figure 3. Image of latest threats within cybersecurity from Trellix*

**

*Figure 4. Image of CaddyWiper malware threat in detail (CaddyWiper Malware Targets Ukraine, seen in figure 3)*

1.5 Recent Threats

With Bank of Ireland catering to over 2 million customers (Bank of Ireland 2022a) the potential of data breaches as a result of cyber threats could result in massive losses for the company. In 2020, Bank of Ireland was fined €1.66 million due to a regulatory breach. This stemmed from an attacker hacking one of the customers’ email account several years ago. However, the institution failed to report this in a timely manner, potentially leaving the company to an even greater vulnerability (Brennan 2022). With this in mind, it is important to highlight the most relevant cyber threats to a financial institution in efforts to safeguard against them.

For the purposes of this report when looking at threats, qualitative risk analysis will be used. This form of analysis is a simpler, subjective methodology and doesn’t require extensive IT experience, meaning staff not necessarily involved in security can be included which will benefit Bank of Ireland’s entire staff with regards to increasing security awareness (Tunggal 2021). The labelling used for threats will be high, medium and low risk. When considering the level of risk this report also takes into consideration the potential impacts of Bank of Ireland’s reputation, especially with past data breaches that have resulted in large fines (O’Donovan 2022).

1. Distributed Denial of Service (DDos):
   * DDos should be placed as high risk. As Bank of Ireland offer a 24-hour, 365-day online banking service the risk of this threat is high.
   * This is an external type of threat given where attackers will attempt to externally get access to the website.
   * DDos attacks work by overwhelming a sever with an abundance of traffic. There can be several forms of this attack such as network, application and amplification attacks (Neil 2020, p.270-271).
   * A flood guard can be implemented into a switch as a preventative measure to DDos attacks by stopping Media Access Control flooding (Neil 2020, p.173).
2. Smishing:
   * Smishing should be placed as medium risk. Though a very common attack with potential for high impacts on business, Bank of Ireland has taken appropriate mitigation measures and is involved with FraudSMART, a company involved in raising fraud awareness (Bank of Ireland 2022c).
   * This is a type of social engineering attack that poses a particular threat to banking customers.
   * Smishing works by attackers pretending they are associated with Bank of Ireland. These attackers focus on contacting customer’s on their phones by sending seemingly legitimate texts containing links to insecure websites prompting you for your personal banking details (Bank of Ireland 2022d).
   * Removing the threat of smishing can be promoted through reminding customer’s that Bank of Ireland will never request for a link to be clicked through text messages that directs you to a website prompting you for your details.
3. Keylogger:
   * With this type of attack becoming more common, specifically with banking applications the risk should be placed as high (Blegen 2021).
   * This is a type of spyware that banking institutions must be particularly aware of due to potentially serious breaches of sensitive data.
   * Keyloggers can record individual keystrokes that a customer may input on a mobile or desktop device. This attack poses a serious threat to Bank of Ireland as a customer’s banking details could be recorded.
   * Pre-emptive measures employees can take to remove the threat of this attack is to ensure all software is up to date with the appropriate security features. Avoiding clicking on any links or attachments that seem suspicious even if sent from other Bank of Ireland staff members. Real-time software that have security features to prevent malicious files from being installed onto the institutions’ devices is also imperative (Malwarebytes 2022).
4. Trojan Horses (Banker Trojan in this context):
   * This type of attack poses a threat specifically to mobile banking. Though decreasing in frequency, attackers are creating more sophisticated versions of it, targeting banks (Osborne 2022). The risk should be placed as medium.
   * This attack is a type of malware that is very popular amongst attackers in banking.
   * Once installed onto a device, trojan’s appear as genuine, legitimate programs. Appearing as a genuine, legitimate program, once installed a trojan can execute malicious operations. Security features on a device can be bypassed and disabled, such as anti-malware software.
   * As trojan’s can prevent a user from uninstalling it, it is important that where a staff member suspects their device may have a trojan installed, said device should be restarted and booted into safe mode. This mode will allow the user to remove the trojan files (McAfee 2020).
5. Man in the Middle:
   * This attack can have a severe impact on a banking institution. Not only can sensitive banking details be accessed but even transactions can be modified, including the amount withdrawn or transferred. The risk should be placed as high.
   * This attack is a derivative of wiretapping attacks (CSRC 2022).
   * In the context of banking, criminals execute this attack by hijacking the connection from Bank of Ireland’s servers and the users mobile or desktop device. Through hijacking this connection, the criminal can access sensitive banking details as well as manipulate banking transactions (Vergara 2022).
   * It is recommended that Bank of Ireland warn customers to use mobile data over public internet/Wi-Fi in scenarios where they may be performing bank transactions. Promoting the use of a VPN is also an appropriate measure in reducing the likelihood of criminals successfully performing this attack (Irwin 2021).
6. Jackpotting:
   * With Bank of Ireland having 250 branches and 2 million customers (Bank of Ireland 2022e), many access its ATM’s daily. This type of attack takes advantage of both software and hardware vulnerabilities associated with these machines. This can result in large sums of money being stolen and therefore poses a relatively high risk. Therefore, the risk should be placed as high.
   * This is a type of logical ATM attack.
   * One form of this attack involves malware. The criminal needs to have access to the ATM itself. Once having access to the machine, a USB stick will be inserted. This USB contains malware that will cause the ATM to dispense cash (Amado 2021).
   * Though this type of attack poses a high risk, an appropriate measure to circumvent this is to ensure all Bank of Ireland branches have security cameras placed with few blind spots, as well as having the ATM placed where members of staff can see who is accessing it. This is effective as these criminals require physical access to these machines. Ensuring anti-malware software is up to date is essential in combatting these attacks (Albright 2018).
7. Credential Stuffing:
   * With many data breaches as of late in Ireland, customers’ usernames and passwords may be leaked from other sources not necessarily associated with Bank of Ireland. However, many people reuse passwords, and it is possible that they may be identical to a customer’s 365 online password. This risk should be placed as medium.
   * Credential stuffing is a derivative of the brute force attack (Mueller 2022).
   * Attackers will deploy bots using these leaked usernames and passwords and attempt to login to a customer’s account.
   * To circumvent this attack, using a combination of authentication methods such as ReCaptcha and sending approval requests via the Bank of Ireland mobile app are appropriate (Raymer 2020).
8. Phishing:
   * This is a common attack that has been highlighted by the Bank of Ireland in detail. However, some customers, particularly elderly customers are vulnerable to these types of attacks (AgeUK 2022). This risk should be placed as high.
   * Phishing is a type of social engineering attack with an emphasis on using emails to reach their victims.
   * Attackers can send emails to customer’s pretending to work on behalf of Bank of Ireland. The customer will be prompted to either click a link or open an email attachment. These links may direct the customer to a website that looks very similar to the Bank of Ireland site and trick them into believing it is legitimate. Attachments often contain malware and will install itself onto the users’ device once downloaded.
   * Being a type of social engineering attack, it is important for Bank of Ireland to inform customers that these attackers take advantage of customers through psychology and attempt to panic them into entering their banking details on these fake websites or by downloading malicious attachments. If customers are aware of common traits in these types of emails, they will be less prone to becoming victims (ITgovernance 2022a).

1.6 Ransomware in online banking attacks

Given that banks deal with very sensitive user data they are an ideal target for attackers. Due to banks holding such data, breaches can result in massive losses for the company, with very large fines as previously mentioned in this report. Therefore, it is understandable that banks may pay off ransoms in order to prevent this data from being leaked but also due to banks not being able to afford having their systems be unavailable, especially when considering the likes of Bank of Ireland’s 365, 24-hour online banking.

Ransomware is a type of malware that weaponizes cryptography concepts for encryption. This is encryption is used to prevent an entity’s data from being accessed. When attackers have successfully seized an entity’s data, they will demand a ransom in order to release it back to them. The scope of the data seized can range from files to databases to applications (McAfee 2022). In 2021, banks saw a 1318% increase in ransomware attacks alone (Henriquez 2021). This increase indicates the need for more appropriate security measures to be implemented.

Pre-emptive measures can be put in place to try avoid ransomware attacks, similar to measures mentioned above such as ensuring all software is up-to-date, not clicking on any link or attachment that seems suspicious, using a VPN and ensuring there is an appropriate backup plan in place.

## Task 2

2.1 Footprinting and its methods

Footprinting relates to collecting information about an organisation’s infrastructure, networks and system. This information acts as the first step in creating a plan to attack an organisation. Essentially, you need to know the internals of an organisation in order to adequately identify vulnerabilities to take advantage of. Examples of information that can be collected through this technique are (Ghahrai 2019):

* Phone numbers
* Computer and web server operating systems
* Domains and subdomains
* Staff members’ details
* Organisation’s geographical locations
* IP addresses

There are several methods that can be used in order to retrieve information about an organisation. Such methods include:

* Search Engines:
  + Such as Google which can be used to find out information such as Bank of Ireland’s outlets, the 365 online login pages and even the employees (a simple search of ‘Bank of Ireland employees’ displays a list of linkedin profiles of said employees, this information alone could be used by skilled attackers for social engineering purposes). Skilled attackers are capable of using detailed queries to retrieve as much valuable information as possible, known as ‘dorks’.
* Whois
  + This is a query that can be used to collected information regarding an organisation’s information. This query can include information such as domain and subdomain details and what domain server is being used. This query can be used on a Linux distribution or there are websites that can also be used to achieve this, such as ‘who.is’ (WHOIS 2022).
* IP Geolocation
  + Can be used to collect information regarding Bank of Ireland’s locations including ISP and eircodes locating branches within the republic of Ireland, Northern Ireland and the UK. There are a number of tools to facilitate this such as IP2Location (SourceForge 2022).

2.2 Bank of Ireland Vulnerabilities

Through using the search engine alone, it is possible to find out about Bank of Ireland’s cybersecurity shortcomings over the years. For over a decade, the company has failed to implement an appropriate system to provide continued assistance to customers during any technical downtime. What is particularly concerning is that reports had shown such issues were raised with the company since 2008 (Brennan and McGee 2021).

Attackers could exploit this vulnerability by overwhelming the company, for example with a DDos attack in an attempt to disrupt Bank of Ireland’s online services, knowing that the company has a history of particular weakness in this area, potentially resulting in further substantial fines being dealt. Aside from implementing pre-emptive measures for attacks such as DDos which has been discussed previously, Bank of Ireland needs to implement more appropriate backup measures in cases where their services may go down. More specifically, a detailed cybersecurity plans need to be designed regarding effective, scalable backup systems.

Knowing that Bank of Ireland facilitates online banking through a web application, this leads the company vulnerable to cross site request forgery (CSRF) attacks. Relating to the company, this is where an attacker manipulates a customer’s browser into performing operations within a web application that the customer did not do themselves. If a customer is using multiple tabs, they may leave their banking tab open while logged in, leaving room for the attacker to take advantage of this.

The attacker can use this attack to transfer the customer’s funds into their own account. To circumvent this, Bank of Ireland should advise customer’s to immediately logout of the 365 online banking application when no longer being used as well as not allowing browsers like Google to store usernames/ID’s and passwords (Oh 2022).

2.3 Security Policy & Social Networking

Company security policies should implement some form of control over social networking, specifically with regards to its own employees. As previously mentioned, through using a search engine it is possible to find a list of Bank of Ireland’s employees through social media apps like LinkedIn. Through discussing of phishing and smishing, we know that attackers are well versed in human psychology and are able to apply this in social engineering techniques. On apps like LinkedIn, where it is easy to locate Bank of Ireland’s staff, these attackers could pretend to be members of staff themselves and attempt to connect with these legitimate staff members.

These attackers could also pretend to be staff members of other reputable companies and may attempt to get Bank of Ireland employees to give their email address, some people may even upload their CV publicly on their profiles, giving more sensitive information to attackers. With this information, attackers can plan their attack.

It is evident that social networking can leave companies like Bank of Ireland vulnerable. It is essential to implement policies that control the amount of information an employee may give and or display on social media apps such as LinkedIn.

## Task 3

3.1 Social Engineering & its impacts

Companies are constantly implementing intuitive and effective counter measures towards cyber-attacks. One vulnerability that companies struggle to defend against is their own customers. As people, customer’s can be very vulnerable psychologically, some more than others. Knowing this, a large number of attackers take advantage of a type of attack known as social engineering. Social engineering incorporates human psychology alongside technical means to trick customer’s into leaking their sensitive information.

In banking, there is a broad age range of customers, of which contain the elderly. As previously mentioned, the elderly are more vulnerable to being taken advantage of by social engineers. However, it is not just the elderly that are vulnerable, anyone can fall victim to social engineering as there are a variety of different types such as angler phishing, where attackers pretend to be customer assistance accounts on the likes of twitter for example. Honey traps take emotional advantage of vulnerable people, particularly lonely people by pretending to be interested in them romantically in order to trick them into sending them cash (ITgovernance 2022b). These are only some examples, alongside phishing and smishing previously discussed above.

It is possible to prevent angler phishing by confirming if the account is legitimate. In the case of twitter, you can check if the account has a blue tick next to the account name, which means it is legit. With Bank of Ireland, all official social media used can be located on the website (Bank of Ireland 2022). Honey traps can be avoided by reminding customers that if a person is demanding a large sum of money, or frequently asks for small loans they should be cautious and try to understand the persons intentions.

3.2 Good practices for banking authentication

As a bank, Bank of Ireland deals with very sensitive user data. It is quintessential for any banking company to have good practices set in place with regards to authentication. Knowing that passwords are constantly being leaked should be considered when a company implements authentication methods. Many banking companies will only take action in the event it has been discovered that an attacker has stolen a customer’s password. As good practice, banks should focus on preventing passwords from being accessed in the first placed (move from reactive protocols to pre-emptive).

Successfully logging into an account does not necessarily mean the person is the actual customer. To try and confirm that it is the rightful owner of the account, multi factor authentication. Biometric-based authentication should be implemented as a common practice in banking companies. Customers view this form of authentication as being more secure due to not needing to use passwords as fingerprint scanning combined with facial recognition can be used instead. Many customer’s understand that for attackers, attempting to bypass biometric-based authentication would be extremely difficult (Wawrzynski 2022).

3.3 Physical access authentication recommendations

With the banking sector, there is one machine in particular where physical access authentication is paramount, ATMs. As previously mentioned, it is possible for attackers to use jackpotting to gain physical access to an ATM to dislodge money. Unfortunately, despite the pandemic causing a major shift to online banking, ATM theft is still on the rise. Some suggestions for authentication are (Atrey 2017):

* Require the use of the 3-digit CVV number on cards for authentication
* Enforce mandatory bank cards that contain chips which can be used to authenticate the card itself is genuine
* Consider biometric authentication embedded into ATMs (such as finger scanning)
* Implement the use of one-time codes sent to the customer’s mobile phone which must be entered into the ATM before use

These recommendations would be relatively simple for Bank of Ireland to implement to all their ATMs across their branches and potentially could reduce the annual number of ATM based thefts.

# Part 2: Penetration testing

## Task 1

* 1. Metasploit payloads & examples

Exploits are used by cyber criminals in order to take advantage of a target’s vulnerability. These exploits are essentially an array of commands that facilitate access to the target’s system. In Metasploit, there are exploit modules, these are known as payloads. There are several types of payloads (Offensive Security 2022):

* Singles/Stageless payload: Generally larger modules that are standalone, meaning they do not require any other modules to be installed. Examples of this type of payload could include running any specific type of file.
* Stagers: These modules connected the cyber criminal with the victim over the network. Unlike singles, they are generally smaller in size and more stable.
* Stages: Additional files that can provide further functionality/features included in the with the stagers. An example is Meterpreter.

# Part 3: Traffic Analysis

## Task 1

* 1. Wireshark tool

The wireshark tool is open source and facilitates capturing network traffic, displaying it in a user-friendly allowing for IT professionals to discover any cyber attacks more easily. Some examples of attacks that can be identified and highlighted using this tool are (InfosecMatter 2021):

* ICMP flooding (DDos attack)
* VLAN hopping (Whereby a VLAN gets traffic directed to it from another VLAN by an attacker)
* ARP spoofing (Is a derivative of man in the middle attack)

# Bibliography

AgeUK (2022) OLDER PERSON BECOMES FRAUD VICTIM EVERY 40 SECONDS| PRESS RELEASE [online], *Age UK*, available: https://www.ageuk.org.uk/latest-press/articles/2019/july/older-person-becomes-fraud-victim-every-40-seconds/ [accessed 2 Mar 2022].

Albright, P. (2018) ‘ATM Jackpotting: How to Protect Your Machines’, *PaymentsJournal*, available: https://www.paymentsjournal.com/atm-jackpotting-how-to-protect-your-machines/ [accessed 30 Mar 2022].

Amado, J. (2021) ‘Hitting the “Jackpot” With ATMs’, *Sepio*, available: https://sepiocyber.com/blog/atm-jackpotting-attack/ [accessed 30 Mar 2022].

Atrey, P. (2017) How Secure Are Today’s ATMs? 5 Questions Answered [online], *The Conversation*, available: http://theconversation.com/how-secure-are-todays-atms-5-questions-answered-79618 [accessed 30 Mar 2022].

Bank of Ireland (2021) ‘Data Privacy Notice: How we manage your personal data’, available: https://www.bankofireland.com/app/uploads/assets/Data-Privacy-Notice-November-2021-Digital.pdf [accessed 20 Mar 2022].

Bank of Ireland (2022a) Bank of Ireland Overview – Investor Relations [online], *Bank of Ireland Overview*, available: https://investorrelations.bankofireland.com/about-us/bank-of-ireland-overview/ [accessed 20 Mar 2022].

Bank of Ireland (2022b) Features of 365 Online Banking - Online Banking - Bank of Ireland [online], *https://personalbanking.bankofireland.com/*, available: https://personalbanking.bankofireland.com/ways-to-bank/online-banking/features-of-365-online-banking/ [accessed 20 Mar 2022].

Bank of Ireland (2022c) Security Zone - Bank of Ireland Group Website [online], *https://www.bankofireland.com/*, available: https://www.bankofireland.com/security-zone/ [accessed 30 Mar 2022].

Bank of Ireland (2022d) Suspicious Texts (Smishing) - Bank of Ireland Group Website [online], *https://www.bankofireland.com/*, available: https://www.bankofireland.com/security-zone/fraudster-tactics/suspicious-texts/ [accessed 30 Mar 2022].

Bank of Ireland (2022e) Branch Listings - Bank of Ireland Group Website [online], *https://www.bankofireland.com/*, available: https://www.bankofireland.com/branch-listing/ [accessed 30 Mar 2022].

Bank of Ireland (2022) Twitter - Social Media - Bank of Ireland [online], *https://personalbanking.bankofireland.com/*, available: https://personalbanking.bankofireland.com/ways-to-bank/social-media/twitter/ [accessed 30 Mar 2022].

Blegen, T. (2021) ‘Keylogger attacks on banking apps increase’, *Promon*, available: https://promon.co/security-news/keylogger-attacks-on-banking-apps-increase/ [accessed 30 Mar 2022].

Brennan, J. (2022) Bank of Ireland Fined €1.66m for Failings amid Cyber Fraud [online], *The Irish Times*, available: https://www.irishtimes.com/business/financial-services/bank-of-ireland-fined-1-66m-for-failings-amid-cyber-fraud-1.4315693 [accessed 30 Mar 2022].

Brennan, J. and McGee, H. (2021) Bank of Ireland Fined €24.5m over IT Flaws [online], *The Irish Times*, available: https://www.irishtimes.com/business/financial-services/bank-of-ireland-fined-24-5m-over-it-flaws-1.4744911 [accessed 30 Mar 2022].

CSRC (2022) Man-in-the-Middle Attack (MitM) - Glossary | CSRC [online], *NIST*, available: https://csrc.nist.gov/glossary/term/man\_in\_the\_middle\_attack [accessed 30 Mar 2022].

Ghahrai, A. (2019) Footprinting and Reconnaissance [online], *DevQA*, available: https://devqa.io/footprinting-overview/ [accessed 30 Mar 2022].

Henriquez, M. (2021) Banking Industry Sees 1318% Increase in Ransomware Attacks in 2021 [online], *Security*, available: https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021 [accessed 30 Mar 2022].

InfosecMatter (2021) Detecting Network Attacks with Wireshark [online], *InfosecMatter*, available: https://www.infosecmatter.com/detecting-network-attacks-with-wireshark/ [accessed 11 Apr 2022].

Irwin, L. (2021) How to Defend against Man-in-the-Middle Attacks [online], *IT Governance Blog En*, available: https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks [accessed 14 Apr 2022].

IT Security Guru, T. (2018) ‘About Us’, *IT Security Guru*, available: https://www.itsecurityguru.org/about-us/ [accessed 30 Mar 2022].

ITgovernance (2022a) Phishing [online], available: https://itgovernance.co.uk/phishing [accessed 30 Mar 2022].

ITgovernance (2022b) What Is Social Engineering? | Techniques & Prevention [online], *IT Governance*, available: https://itgovernance.co.uk/social-engineering-attacks [accessed 30 Mar 2022].

Jackson Higgins, K., Rashid, F., Donahue, J., Spiegelman, K., Kesten, G., Chickowski, E., Lemos, R., Vijayan, J., and Zuerier, S. (2022) About Us, Contact Us [online], *Dark Reading*, available: https://www.darkreading.com/about-us [accessed 22 Mar 2022].

Malwarebytes (2022) What Is a Keylogger? | How to Detect Keyloggers [online], *Malwarebytes*, available: https://www.malwarebytes.com/keylogger [accessed 30 Mar 2022].

McAfee (2020) ‘Understanding Trojan Viruses and How to Get Rid of Them’, *McAfee Blog*, available: https://www.mcafee.com/blogs/internet-security/understanding-trojan-viruses-and-how-to-get-rid-of-them/ [accessed 30 Mar 2022].

McAfee (2022) What Is Ransomware? | McAfee [online], *McAfee*, available: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html [accessed 30 Mar 2022].

Mueller, N. (2022) Credential Stuffing Software Attack | OWASP Foundation [online], *OWASP*, available: https://owasp.org/www-community/attacks/Credential\_stuffing [accessed 30 Mar 2022].

Neil, I. (2020) *CompTIA Security+: SY0-601 Certification Guide*, Second. ed, Packt Publishing.

O’Donovan, B. (2022) Bank of Ireland Fined €463,000 for Data Breaches [online], *RTÉ*, available: https://www.rte.ie/news/business/2022/0405/1290503-bank-of-ireland-fined-by-dpc/ [accessed 30 Mar 2022].

Offensive Security (2022) ‘Understanding Payloads in Metasploit | Offensive Security’, available: https://www.offensive-security.com/metasploit-unleashed/payloads/ [accessed 1 Apr 2022].

Oh, J. (2022) ‘What is CSRF | Cross Site Request Forgery Example | Imperva’, *Learning Center*, available: https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/ [accessed 30 Mar 2022].

Osborne, C. (2022) Almost 100,000 New Mobile Banking Trojan Strains Detected in 2021 [online], *ZDNet*, available: https://www.zdnet.com/article/almost-100000-new-mobile-banking-trojans-detected-in-2021/ [accessed 30 Mar 2022].

Raymer, W. (2020) Credential Stuffing: What Banks Need to Know [online], *BAI*, available: https://www.bai.org/banking-strategies/article-detail/credential-stuffing-what-banks-need-to-know/ [accessed 30 Mar 2022].

Sheridan, K. (2022) FireEye & McAfee Enterprise Renamed as Trellix [online], *Dark Reading*, available: https://www.darkreading.com/threat-intelligence/fireeye-mcafee-enterprise-renamed-as-trellix [accessed 30 Mar 2022].

SourceForge (2022) IP2Location [online], *SourceForge*, available: https://sourceforge.net/software/product/IP2Location/ [accessed 30 Mar 2022].

The Hacker News (2022) About ‘The Hacker News’ — Cybersecurity Publication [online], *The Hacker News*, available: https://thehackernews.com/p/about-us.html [accessed 22 Mar 2022].

Trellix (2022) Trellix Threat Center – Latest Cyberthreats | Trellix [online], *The latest cybersecurity threats*, available: https://www.trellix.com/en-us/threat-center.html [accessed 30 Mar 2022].

Tunggal, A.T. (2021) IT Security Risk Assessment Methodology: Qualitative vs Quantitative | UpGuard [online], *UpGuard*, available: https://www.upguard.com/blog/risk-assessment-methodology [accessed 30 Mar 2022].

Vergara, D. (2022) How Banks Can Combat Man in the Middle Attacks [online], *OneSpan*, available: https://www.onespan.com/blog/banks-combat-man-in-the-middle-attacks [accessed 30 Mar 2022].

Wawrzynski, M. (2022) The Need for Advanced Authentication: Why Banks and FIs Should Consider an Upgrade of Their Authentication Methods [online], *THE PAYPERS*, available: https://thepaypers.com/expert-opinion/the-need-for-advanced-authentication-why-banks-and-fis-should-consider-an-upgrade-of-their-authentication-methods--1253902 [accessed 30 Mar 2022].

WHOIS (2022) WHOIS Search, Domain Name, Website, and IP Tools - Who.Is [online], *who.is*, available: https://who.is/ [accessed 30 Mar 2022].