**Week 3 Assignment**

**RECENT INCIDENTS, THEIR CAUSES, AND IMPACTS**

**1. LoanDepot Ransomware Attack (January 2024):**

* **Cause:** In January 2024, LoanDepot, a major mortgage lender, fell victim to a ransomware attack that exposed the sensitive data of approximately 16.9 million customers, including Social Security numbers, account numbers, names, addresses, and other data. ​[secureframe.com](https://secureframe.com/blog/recent-cyber-attacks)
* **Impact:** The breach led to unauthorized access to personal and financial information, resulting in significant operational disruptions and financial losses.​

**2. MOVEit Data Breach (June 2023):**

* **Cause:** A vulnerability in MOVEit, a managed file transfer software, was exploited by the Cl0p ransomware group. ​
* **Impact:** This breach impacted thousands of organizations, including the BBC, British Airways, and U.S. government agencies, compromising sensitive data of millions.​

**3. Change Healthcare Ransomware Attack (February 2024):**

* **Cause:** In February 2024, Change Healthcare, a U.S. healthcare technology company, suffered a ransomware attack that disrupted medical services nationally and impacted over 100 million people's data. ​[crn.com+2wired.com+2axios.com+2](https://www.wired.com/story/worst-hacks-2024)
* **Impact:** The attack caused massive disruption in the U.S. healthcare system for weeks, affecting the delivery of medical services and compromising sensitive patient information.​[crn.com](https://www.crn.com/news/security/2024/10-major-cyberattacks-and-data-breaches-in-2024-so-far)

**4. Services Australia Data Breaches (September 2024):**

* **Cause:** Services Australia experienced a substantial increase in data breaches, primarily due to scammers using stolen information from previous hacks to access customer accounts. ​[theguardian.com](https://www.theguardian.com/australia-news/2024/sep/29/services-australia-hacks-data-breach-scam)
* **Impact:** The surge in breaches led to unauthorized access to customer accounts, resulting in potential identity theft and fraud.​[theguardian.com](https://www.theguardian.com/australia-news/2024/sep/29/services-australia-hacks-data-breach-scam)

**5. T-Mobile Data Breach (2021):**

* **Cause:** In 2021, T-Mobile suffered a data breach that exposed the personal information of over 40 million customers. ​[electric.ai](https://www.electric.ai/blog/recent-big-company-data-breaches)
* **Impact:** The breach led to unauthorized access to customer data, resulting in potential identity theft and fraud.​

**6. Equifax Data Breach (2017):**

* **Cause:** In 2017, Equifax, a major credit reporting agency, experienced a breach due to a failure to patch a known vulnerability in Apache Struts software. ​
* **Impact:** The breach exposed personal information of approximately 147.9 million Americans, 15.2 million British citizens, and 19,000 Canadians, leading to widespread identity theft concerns.​

**7. Capital One Data Breach (2019):**

* **Cause:** In 2019, Capital One suffered a data breach due to a misconfigured firewall in its cloud infrastructure. ​
* **Impact:** The breach exposed personal information of over 100 million customers, including credit scores, credit limits, and payment history.​

**8. Twitter Data Breach (2020):**

* **Cause:** In 2020, Twitter experienced a data breach due to a social engineering attack targeting employees. ​
* **Impact:** The breach led to unauthorized access to high-profile accounts, including those of Elon Musk and Barack Obama, resulting in potential misinformation and fraud.​

**Common Causes of Cybersecurity Breaches:**

* **Unpatched Vulnerabilities:** Failure to update software and systems can leave them open to exploitation.​
* **Ransomware Attacks:** Malware that encrypts data, demanding payment for decryption.​
* **Insider Threats:** Employees or contractors intentionally or unintentionally compromising security.​
* **Phishing Attacks:** Deceptive communications tricking individuals into revealing sensitive information.​

**Impacts of Cybersecurity Breaches:**

* **Financial Losses:** Costs related to incident response, legal fees, and potential fines.​
* **Reputational Damage:** Loss of customer trust and damage to brand reputation.​
* **Legal Consequences:** Potential lawsuits and regulatory penalties.​
* **Operational Disruptions:** Interruption of services and business operations.

Steps to Identify Phishing Emails Using Free Online Tools:

1. Examine the Email Manually (Initial Red Flags)

common phishing indicators to look for before using tools,

* Sender Email Address: Check if it’s from *support@safebank.com* or something like *support@saf3bank.com* or *safebank-support@randomdomain.com*. Phishers often use slightly altered or unrelated domains.
* Urgent or Threatening Language: Phrases like “Act now or your account will be closed” or “Verify immediately” are common in phishing emails.
* Links: Hover over any links (without clicking) to see the URL. If it leads to a domain like secure-login-update.com instead of safebank.com, it’s suspicious.
* Spelling/Grammar Errors: Look for typos or awkward phrasing, though modern phishing emails (using AI) might have perfect grammar.
* Generic Greetings: If the email says “Dear Customer” instead of your name, it could be a red flag.

In this simulation, let’s say the sender *is notifications@safebank-security.net*, the link is *https://secure-login-update.com/verify*, and the tone is urgent.

