RECENT CYBERSECURITY BREACHES, THE CAUSES AND IMPACTS

1. Genea IVF Clinic Ransomware Attack (February 2025)

- **Cause:** The Australian IVF clinic Genea was targeted by the ransomware group "Termite," leading to unauthorized access to their systems.
- **Impact:** The attack disrupted phone lines, interfered with IVF cycles, and resulted in nearly a terabyte of sensitive patient data being leaked on the dark web. The breach underscored vulnerabilities in healthcare data security and raised concerns about the adequacy of existing privacy laws in Australia.

2. Polish Space Agency Cyberattack (March 2025)

- **Cause:** Unauthorized access was detected within the IT infrastructure of the Polish Space Agency (POLSA). While specific details about the perpetrators remain undisclosed, the breach is under investigation.
- **Impact:** In response to the intrusion, affected systems were secured, and intensive efforts are underway to identify those responsible. This incident highlights the persistent threats faced by governmental agencies, especially in sectors critical to national interests.

3. AT&T Data Breach (March 2024)

- **Cause:** Hackers infiltrated AT&T's systems, compromising personal data of both current and former customers.
- **Impact:** The breach affected approximately 7.6 million current and 65.4 million former customers, exposing sensitive information such as Social Security numbers, account details, and passcodes. This incident raised significant concerns about data security practices within major telecommunications companies.

4. Rise in Business Email Compromise (BEC) Scams (2023)

- **Cause:** Cybercriminals increasingly targeted businesses by exploiting vulnerabilities in email systems, often using AI to craft convincing fraudulent communications.
- **Impact:** In 2023, BEC scams resulted in losses estimated at $2.9 billion. Companies faced financial damages averaging $137,000 per

incident. The sophistication of these attacks, including the creation of fake email threads and websites, posed significant challenges for corporate cybersecurity defenses.

Common Causes of Cybersecurity Breaches:

- **Human Error:** A significant portion of breaches are attributed to human mistakes, such as falling for phishing scams or misconfiguring systems.
- **Malware and Ransomware:** Malicious software continues to be a prevalent method for attackers to gain unauthorized access and disrupt operations.
- **Phishing Scams:** Deceptive communications designed to trick individuals into revealing sensitive information remain a common attack vector.

Impacts of Cybersecurity Breaches:

- **Financial Loss:** Breaches often lead to direct financial losses, including theft and costs associated with remediation.
- **Reputational Damage:** Organizations suffer harm to their reputation, leading to loss of customer trust and potential revenue decline.
- **Operational Disruption:** Attacks can disrupt business operations, leading to downtime and reduced productivity.

PHISHING REPORT

Tools Used

Tool Name	**Website Link**	**Purpose**
VirusTotal	https://virustotal.com/	Scan suspicious email attachments or links

PhishTank	https://www.phishtank.com	Check if URLs are listed as phishing websites
Google Safe Browsing	https://transparencyreport.google.com/safe-browsing/search	Verify suspicious website links