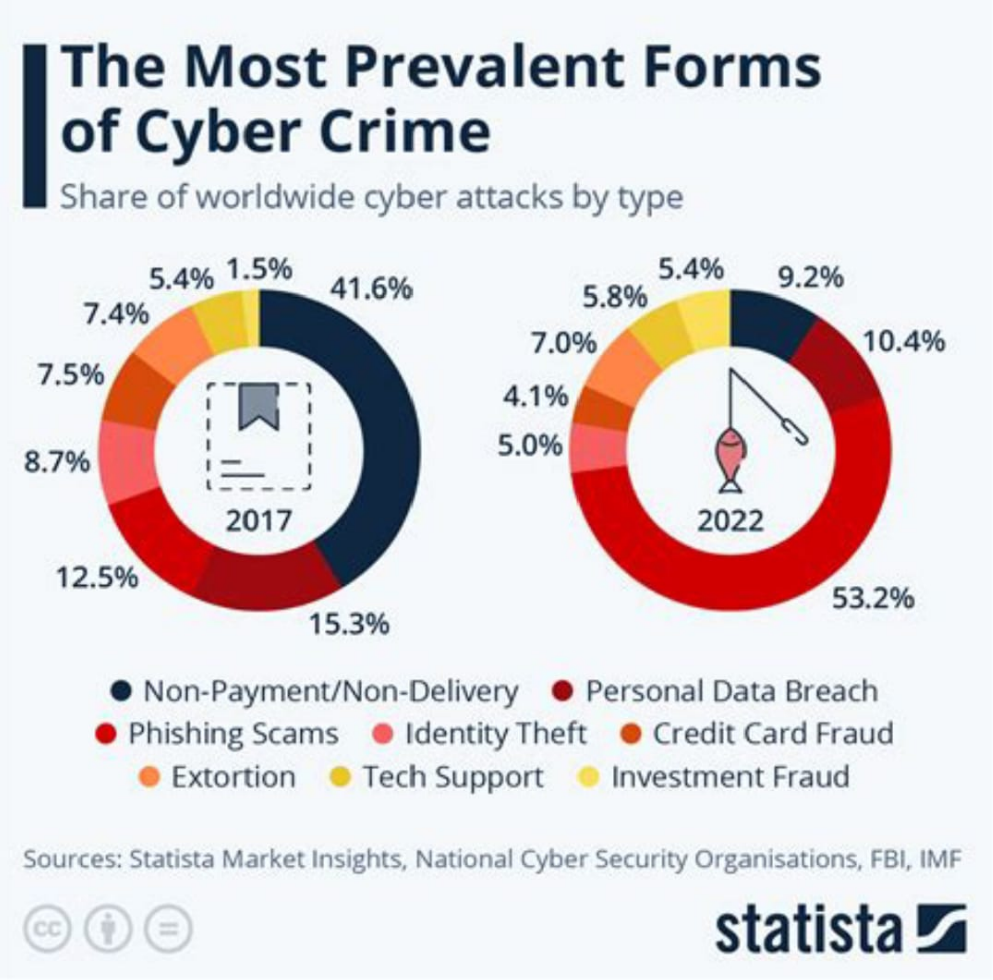
Recent time data hacking news

Bank sepah cyber attack

Introduction:

In March 2025, Iran's financial sector faced a significant cybersecurity breach when the hacker group known as "Codebreakers" claimed responsibility for infiltrating Bank Sepah, one of the country's oldest and most strategically important banks. This incident not only exposed vulnerabilities within Iran's banking infrastructure but also ignited widespread public discourse on financial transparency and governance.(WIKIPEDIA).

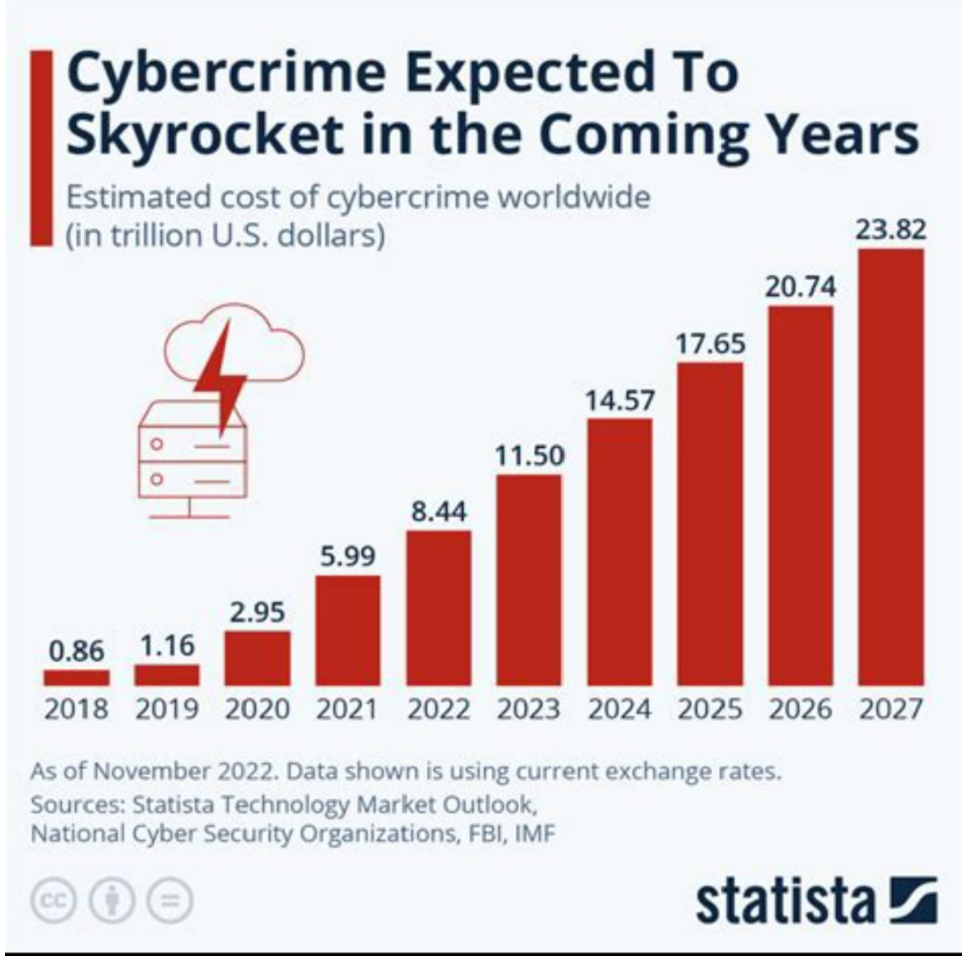
Cyber crime rate



The Most Prevalent Forms of Cyber Crime

Share of worldwide cyber attacks by type

Sources: Statista Market Insights, National Cyber Security Organisations, FBI, IMF



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF

The breach and Its Scope

- The Codebreakers announced their successful cyberattack on Bank Sepah through social media platforms, asserting that they had accessed over 12 terabytes of sensitive data pertaining to more than 42 million customers. The compromised information reportedly included account numbers, passwords, transaction histories, and personal details such as mobile numbers and addresses. Notably, the data also encompassed information related to military personnel and high-ranking officials .(WIKIPEDIA)
- The hackers demanded a ransom of $42 million in Bitcoin, giving the bank a 72-hour window to comply to prevent the public release of the data. Bank Sepah, however, denied any breach, asserting that their systems were secure and disconnected from the internet. Simultaneously, the bank issued warnings to media outlets against disseminating any leaked information, threatening legal action

Public Disclosure and Reaction

In response to the bank's denial, the Codebreakers released portions of the stolen data, revealing the financial details of approximately 20,000 individuals, including prominent figures such as:

- General Hassan Palarak, a former senior commander of the Revolutionary Guards Quds Force, with an account balance of 634 billion tomans (approximately $6.12 million).
- Abbas Golmohammadi, former Deputy Director of Exploration at the Geological and Mineral Exploration Organization, holding 768 billion tomans.
- Alireza Arash, a board member of Henkel Pakwash, with 408 billion tomans.

The revelation of such substantial sums held by individuals closely tied to the military and government sectors sparked outrage among the Iranian populace. Social media platforms were inundated with criticism, questioning the disparity between the wealth of these elites and the economic hardships faced by ordinary citizens. Journalists and academics highlighted the incident as indicative of systemic corruption and a lack of financial transparency within the regime(.WIKIPEDIA)

Broader Implications and Historical Context

This cyberattack is not an isolated incident but part of a series of breaches that have plagued Iran's critical infrastructure in recent years. Notably, in August 2024, a group named IRLeaks targeted multiple Iranian banks, leading to what was described as the "worst-ever" cyberattack on the country's banking system. The Iranian government reportedly paid millions in ransom to prevent the release of sensitive data from over 20 financial institutions.(IFMAT).

The recurring nature of these cyberattacks underscores significant vulnerabilities in Iran's cybersecurity measures, particularly concerning institutions integral to national security and economic stability. The exposure of high-level officials' financial data not only compromises individual privacy but also threatens the integrity of governmental operations.

Conciusion:

The Bank Sepah cyberattack orchestrated by the Codebreakers serves as a stark reminder of the pressing need for robust cybersecurity protocols within Iran's financial institutions. Beyond the immediate technical ramifications, the incident has catalyzed a broader societal reckoning with issues of corruption, transparency, and governance. As Iran continues to navigate the complexities of digital security, the lessons from this breach highlight the critical importance of safeguarding sensitive information and maintaining public trust in financial systems.

REFERANCE

1."Codebreakers attack on Bank Sepah," Wikipedia

2."Hackers Claim Access to 42 Million Sepah Bank Records, Bank Denies Breach," IranWire

3."Iran Pays Millions in Ransom to End Cyberattack on Banks," IFMAT,

4."Data of 20 Iranian banks hacked in 'worst-ever' cyberattack," IFMAT