MAY 2024

3+ Report

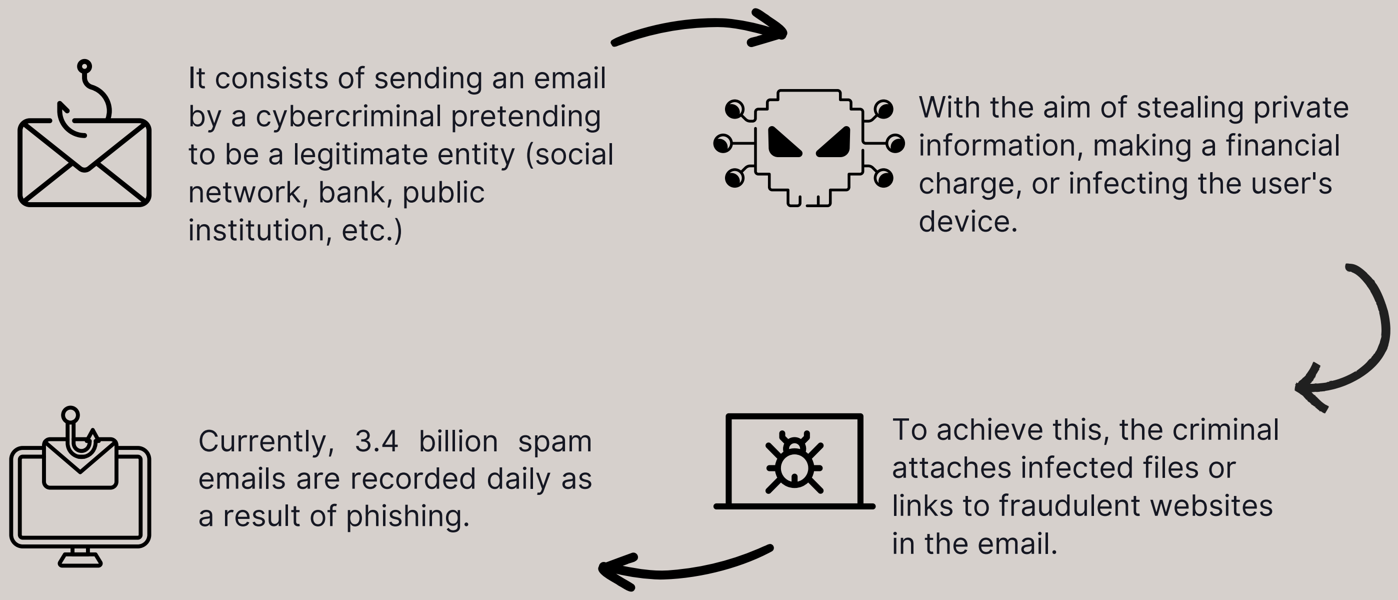
PRIVATE SECURITY ANALYSIS

PHISHING

Cyberattacks are unauthorized accesses to computer systems or networks by third parties. Those who engage in these practices are called cybercriminals or "hackers." They carry out these actions for various purposes, mainly to steal information, manipulate the systems of specific companies or organizations, and demand money in exchange for the restoration of the platforms. Cyberattacks involve the potential breach, loss, or manipulation of data, which results in a negative impact for the victim of the crime.

In 2023, cyberattacks experienced an 87% increase globally, with China, Russia, and Iran being the most affected countries and phishing responsible for 90% of data breaches.
Phishing is one of the most common cyberattacks.

WHAT DOES IT CONSIST OF?



It consists of sending an email by a cybercriminal pretending to be a legitimate entity (social network, bank, public institution, etc.)

With the aim of stealing private information, making a financial charge, or infecting the user's device.

To achieve this, the criminal attaches infected files or links to fraudulent websites in the email.

Currently, 3.4 billion spam emails are recorded daily as a result of phishing.

In Colombia, an average of four phishing attempts per minute have been reported, and it is among the five most commonly materialized cybercrimes.

According to "Kaspersky," a global cybersecurity and digital privacy company

RECOMMENDATIONS

- When receiving an email, make sure you know the sender. If they do not seem familiar, be suspicious of the message. Otherwise, check that the email address is spelled correctly and is the same as the one from which you normally receive emails.
- Do not fill out or provide personal or financial information through forms or surveys sent by email. Banks or companies do not request passwords, usernames, or sensitive product information through any communication channel.
- Avoid accessing banking portals through hyperlinks. Instead, ignore, delete, and report any suspicious message to your bank or organization.
- Check if the email contains grammatical errors. These types of attacks usually have spelling mistakes and unusual vocabulary.
- Do not trust generic subject lines (invoice, receipt, etc.). Ensure that attachments do not have ".js" extensions, as these can bypass antivirus protections.
- Enable the operating system option that allows you to see file extensions. This way, you can check if it is an executable, text document, JavaScript, etc.
- Disable Microsoft Office macros and be cautious with files that ask you to enable them. If you suspect a link included in the email, scrutinize the link carefully.
- Remember to keep your operating system, antivirus, and applications always updated to the latest version.
- Stay constantly informed about new trends in data capture, impersonation, or other criminal methods derived from phishing to be aware of how to act.
- If you believe you have been a victim of phishing, report it to financial institutions, organizations, and interest groups to prevent the spread of other crimes such as fraud, data outsourcing, identity theft, etc.

3securitycol.com