SafetyMails provides a checklist to protect the market — and democracy — from fake emails

In a world where almost half of all email messages sent are fake, SafetyMails warns about the dangers of fake emails and how protection is essential

SafetyMails: fake emails are a danger to people, companies and democracies

RIO DE JANEIRO, RJ, BRASIL, June 25, 2024 /EINPresswire.com/ -- In a world where email communication is massive and fake messages account for almost half of all messages, SafetyMails, email verification service, highlights the importance of identifying and combating fake emails to guarantee the security of people, companies — and even democratic processes.

Fake emails can take many forms, aiming to forge real situations in email messages in order to involve the recipient in actions that could harm them.

The goal of fake email senders is to take advantage of their victims, through deception, data theft, fraud and blackmail.

Fake email can damage people, companies and democracies

For individuals, fake emails can lead to significant financial losses, either through scams or malicious software. Passwords for email accounts, social networks and credit card details are among the main targets.

Companies are targeted by spammers, who seek to steal passwords or hack into databases and servers, aiming to blackmail these companies in order to obtain ransoms, either from encrypted databases, hacked websites or social networks with stolen property, as well as seeking payment, for example, for fake invoices.

Democracies can also suffer. Just as fake news today is part of social networks and messaging

apps, through malicious posts and shares with fake videos and audios and even forged by artificial intelligence, in the email universe, it is a channel that can quickly deliver false information to specific target groups.
With the dissemination of false information, the goal is to manipulate public opinion, leading to impacts on electoral results for or against a particular candidate, in any sphere of democracy.

What is the purpose of each type of email fake?

Some of them are the way the texts are written, how the layout is created (to look like that of a bank, for example), with the way these emails identify their senders (using email addresses similar to the real ones), or even using email accounts that become impossible to contact and trace after a while (known as temporary emails).

The main types of fake email are:
- Phishing: an email that disguises itself to look like a legitimate source, such as a bank or e-commerce.
- Whaling: a phishing email that targets decision-makers in companies, demanding to talk about urgent executive or critical legal issues.
- Scam: fraud emails aimed at convincing recipients to send money, make online payments or obtain financial advantages in exchange for money.
- Malware: emails that contain links or files infected with malicious software that can steal data such as passwords, credit card numbers, among others.
- Spam: emails that force unwanted sales or provide false information.
- Temporary emails: sometimes people can use legitimate temporary email services for illicit purposes, without leaving any trace of their actions SafetyMails suggests that companies use email verification services, including in registration forms, removing and preventing this type of email address from their lists).

How to identify and avoid a fake email

The first step to avoiding these types of emails is to know the more specific characteristics of each one.

Basically, there are 10 main aspects that can help you to identify, almost immediately, whether an email is the vehicle of a scam attempt. When you recognize any abnormal characteristics, we recommend ignoring and deleting the email message as soon as possible.

Look for grammatical errors, strange links (usually shortened), unsolicited attachments, messages with unrealistic promises such as enrichment and unmissable opportunities. Also, run away from emails whose messages make exaggerated mention of the urgency for an action to be taken, especially those referring to payments.

Having anti-malware software installed is also essential for identifying cyber threats in fake

emails.
You no longer have to fall victim to fake emails and online scams. Follow these information and stay safe.

SafetyMails offers a checklist against fake emails

By visiting the SafetyMails website, you can get more information about fake email and also an online checklist that will assess the risk of an email you have received. There are ten questions about aspects of the email which, when added together, result in a warning score about the risks involved in incoming messages.

About SafetyMails
Created in 2017, SafetyMails is an email Verification service for email lists and registration forms — www.safetymails.com

Priscila Gonçalves
SafetyMails
press@safetymails.com
