SMARTFENSE

Disarming Cybercriminals

Free tools to prevent Social Engineering attacks

Introduction

Cybercriminals have a wide variety of techniques in their arsenal to carry out their social engineering attacks.

That's why we, at **SMARTFENSE**, have developed a **series of free tools to improve your defense**.

If you act proactively, cybercriminals will find it very difficult to perpetrate attacks on your organization.

From **SMARTFENSE**, we recommend addressing Information Security through **layers of protection**, being **awareness a fundamental factor** to reduce the risk of your users becoming victims of a Social Engineering attack.

CEO Fraud

A cybercriminal can send emails to users in your organization **impersonating a high-ranking person** and exploit their influential position to make fraudulent requests.

If the corporate email server **is not properly configured**, a cybercriminal can send emails on behalf of a senior executive from the organization's own server, bypassing security controls such as **SPAM** filters or **SPF**, **DKIM**, and **DMARC** records.

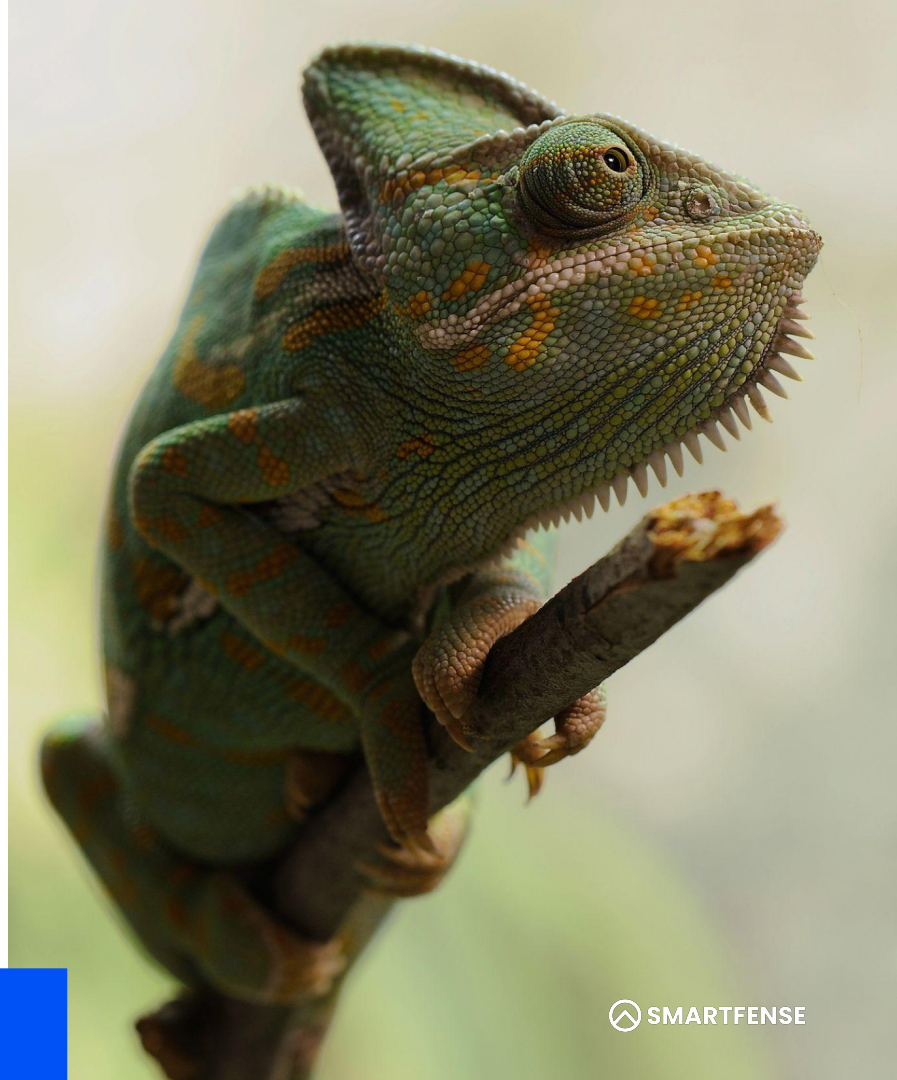
- Discover if your mail server is vulnerable and close this door to cybercriminals!

Spoof Check

If your organization's domain is not properly protected, a cybercriminal can use it to send emails. To protect your domain correctly, you must implement the following protocols:

- **SPF:** Identify the SMTP servers authorized to send emails in a domain.
- **DKIM:** Add a digital signature to legitimate emails using cryptography.
- **DMARC:** Apply quarantine and rejection policies to emails that do not comply with SPF and DKIM protocols.

- Find out if your domain is protected and prevent its use by cybercriminals!



DNS Twist

Protecting your domain and corporate mail server is essential to fight identity spoofing.

However, this will not stop a cybercriminal. With this protection, the most common option is to use a domain similar to that of your organization.

To mitigate this risk, you should periodically check for registered similar domains and ensure that they belong to legitimate organizations.

- Discover the domains similar to yours and control their use!

Email Harvester

A high percentage of phishing attacks are conducted via email.

A cybercriminal can learn the email addresses of your organization's users and send them phishing emails.

The easiest way to obtain the addresses is by simply looking for those that are exposed on the Internet.

- Find out how exposed your organization's email accounts are and raise awareness among the users who use them!

Thank You

www.smartfense.com
info@smartfense.com