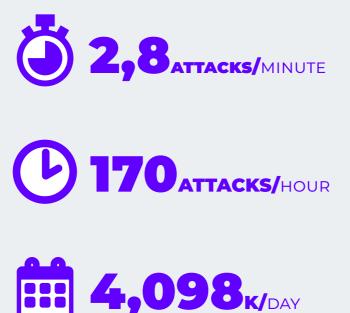## LETTER FROM THE CEO

PHISHING ON THE RISE - DON'T TAKE THE BAIT!

The seventh edition of the Digital Security Report for the United States portrays an alarming number of phishing victims. In 2019, an estimated 19,5 million Americans were victims of cyber attacks. In addition, 33% of the entire Android population received, accessed or shared malicious links related to a "fake promotions or giveaways" theme, creating 6,4K potential victims across the country.

Adware scam was the top strategy used by cybercriminals to spread malicious links in 2019, reaching 1.1 million clicks and shares during the period. Browsers remain the most used platform to spread cyber attacks. In the last year, they accounted for 71% of the total records made by the dfndr lab.

MARCO DEMELLO
CEO of PSafe

VICTIMS BY MALICIOUS URLS

2,8 ATTACKS/MINUTE

170 ATTACKS/HOUR

4,098 K/DAY

19,5 MILLION
Android users are potential victims of **malicious URLs** in the US*

*Projection based on a random sample of 700K American Android users

MAIN DISSEMINATION SOURCES

BROWSERS
71,6%

SMS
23,3%

MESSAGING APPS
4,9%

TYPES OF ATTACKS

Type	%
Fake promotions or giveways	**33%**
Fraudulent advertisements	**24,6%**
Generic malicious links	**20,8%**
Banking payment phishing	**9,5%**
Fake services	**4,5%**
Messenger schemes	**2,6%**
Others**	**28,4%**

19,5 K
Android users potentially affected by **Fake promotions and giveaways** in the US*

*Projection based on a random sample of 700K American Android users

**Fake news, paid mobile services, generic phishing scams, malware downloads, social media phishing.

GOLPES MAIS POPULARES

1: Adware
Malicious sites that allow cybercriminals to send push and spam notifications to the victim and profit from each ad view.

1,1 MILLION CLICKS AND SHARES

2: False draw
The coup promises alleged benefits, saying that to receive them you will need to fill out a form through which you steal victims' personal information.

1 MILLION CLICKS AND SHARES

3: Free gift card
Criminals offer a supposed gift card, saying that to get it you will need to fill out a form through which you steal victims' personal information.

910K CLICKS AND SHARES

CYBERSECURITY REPORT RESEARCH METHODOLOGY

dfndr lab utilizes proprietary artificial intelligence (AI) and machine learning technologies to analyze and detect cyberattacks, the latest malware and viruses, online scams and cyber crime trends.

Approximately 200M digital files are collected daily, evaluated and indexed by dfndr lab's data processing system to keep our products current when it comes to protecting users' devices and staying steps ahead of cybercriminals.

This Cybersecurity Report drew a random sample of 700K Android mobile users who have dfndr security installed. The sample analysis is based on data collected between January 1, 2019 and December 31, 2019.