NormShield

# 2019 H1

## BANKING PHISHING REPORT

Phishing domains pose a significant cyber risk for major banks. Learn how many phishing domains for major banks there are and how to find them.

**To be able to steal sensitive information such as credit card data, hackers create phishing domains impersonating financial institutions to lure their victims. Phishing attacks can create dramatic costs for both customers and organizations. If your employees are exposed to phishing attacks, your entire network and brand are at risk. In addition, attacks on you will cause serious reputation loss.**

## Executive Summary

**50 major banks** around the world are studied in this research.

**1,900+** potential phishing domains are registered in the first half of 2019

**14%** increase in the number of phishing domains when compared to 2018 – H1

**2X** certified potential phishing domains registered compared to ones registered in 2018

## Contents

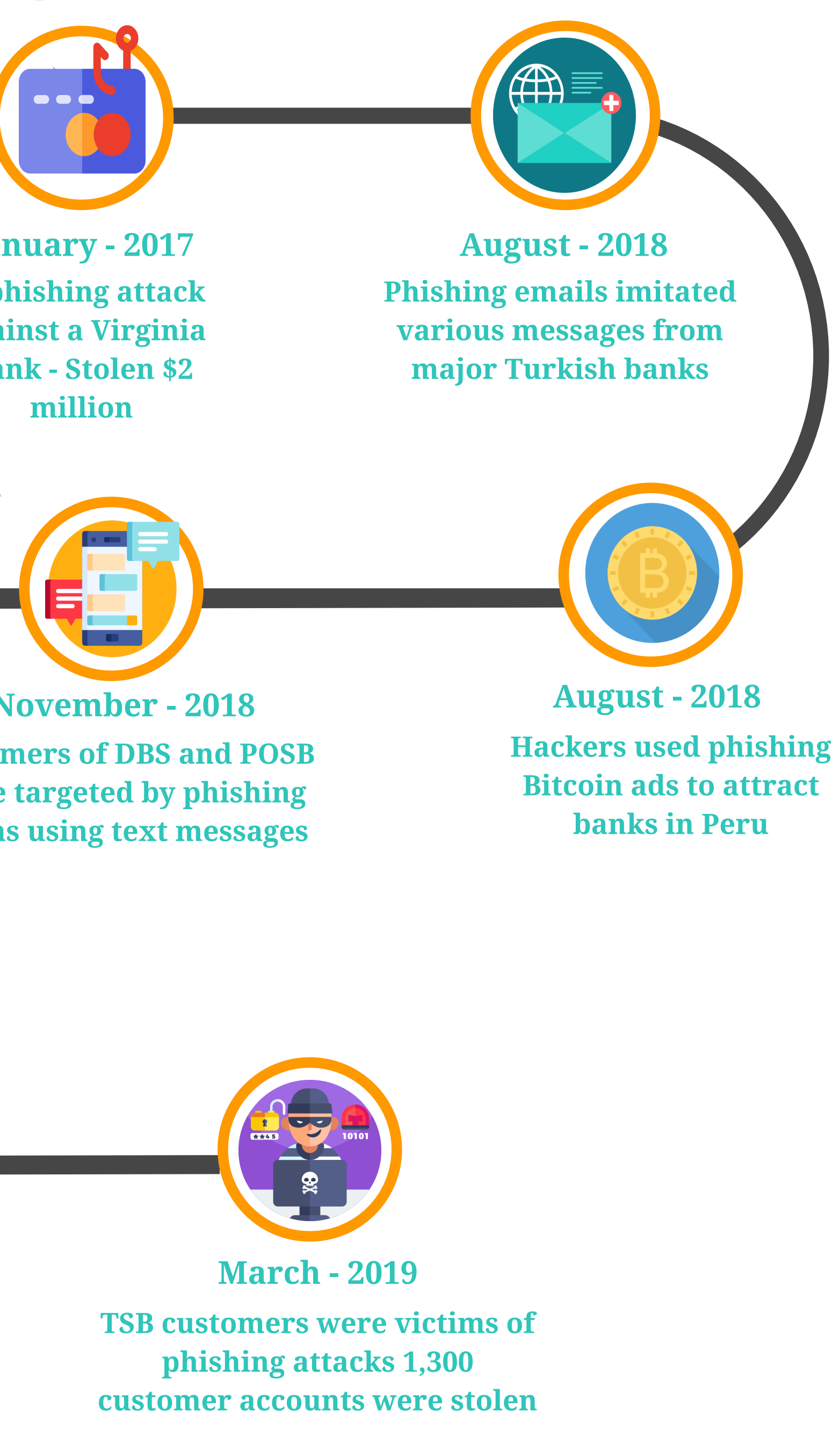
01 Recent phishing attacks against banks
02 Banking phishing domain
03 Phishing domain search
04 Search Tips
05 About Us
06 Let's get in touch

https://www.normshield.com/

## Recent Phishing Attacks Against Banks

**Phishing attacks are now more target oriented**

Adversaries improve their phishing-attack methods to execute advanced attacks against banks. They closely watch the campaigns of banks, the economy of countries, the status of different investment options (e.g., bitcoin), and produce more convincing scenarios.



**January - 2017**
A phishing attack against a Virginia Bank - Stolen $2 million

**August - 2018**
Phishing emails imitated various messages from major Turkish banks

**August - 2018**
Hackers used phishing Bitcoin ads to attract banks in Peru

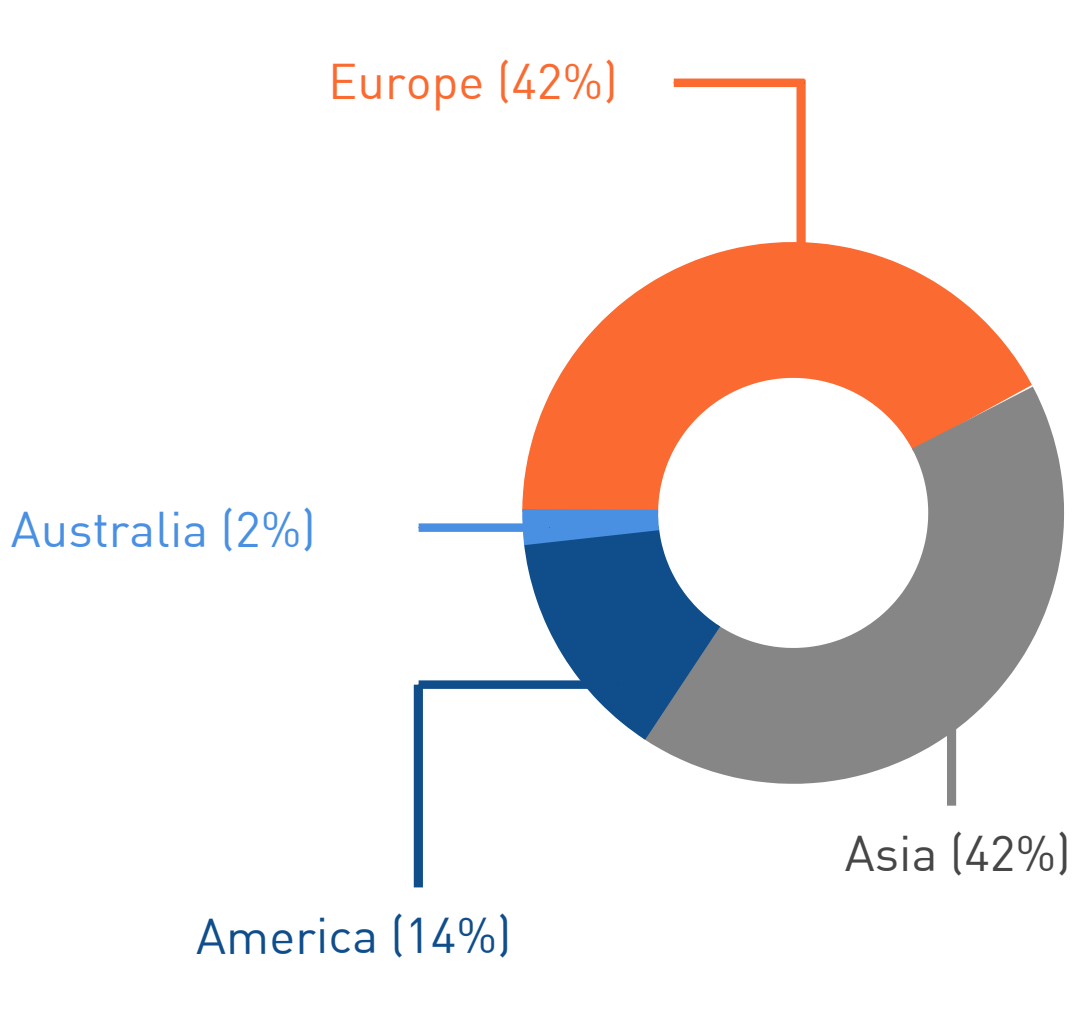
**November - 2018**
Customers of DBS and POSB were targeted by phishing scams using text messages

**January - 2019**
North American banks were imitated using phishing scams to infect victims with TrickBot

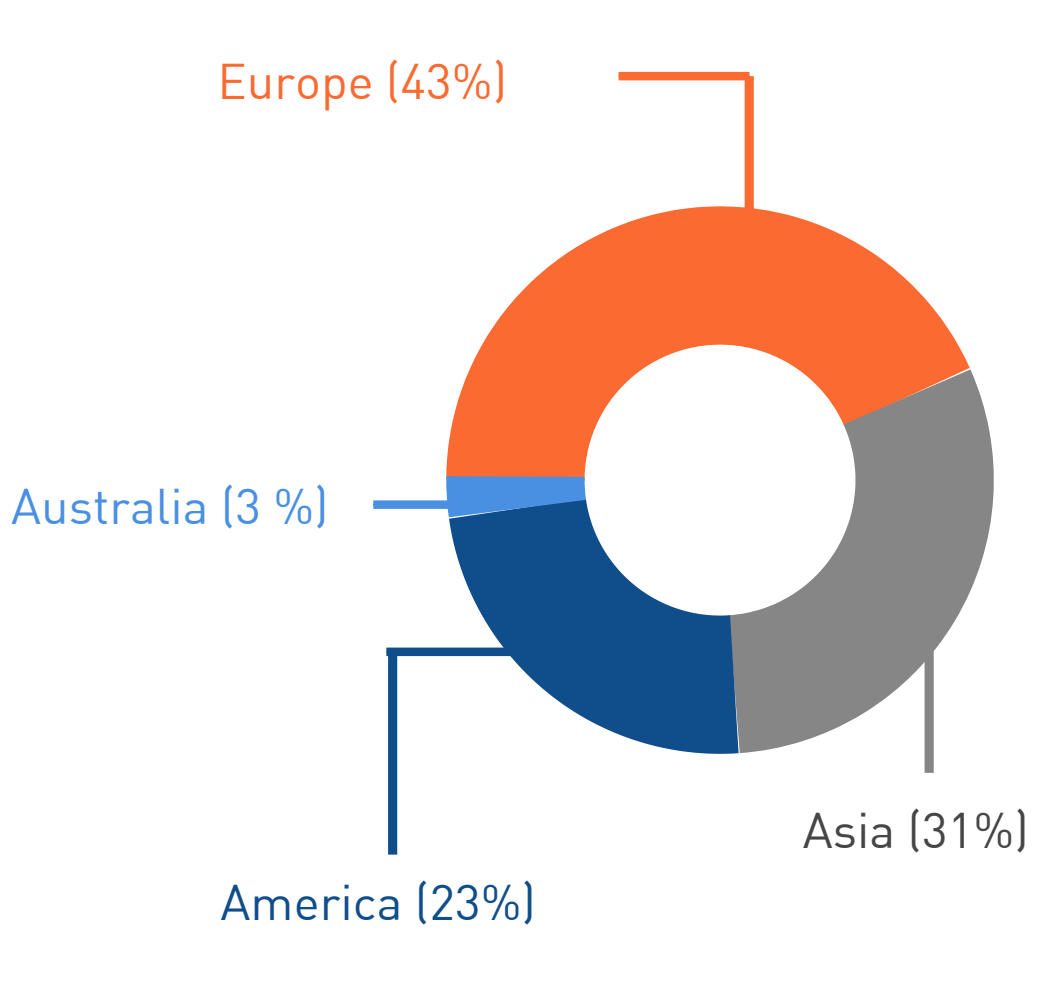
**February - 2019**
Compromised banks are used as a first step of phishing attacks by hackers

**March - 2019**
TSB customers were victims of phishing attacks 1,300 customer accounts were stolen

## Banking Phishing Domain



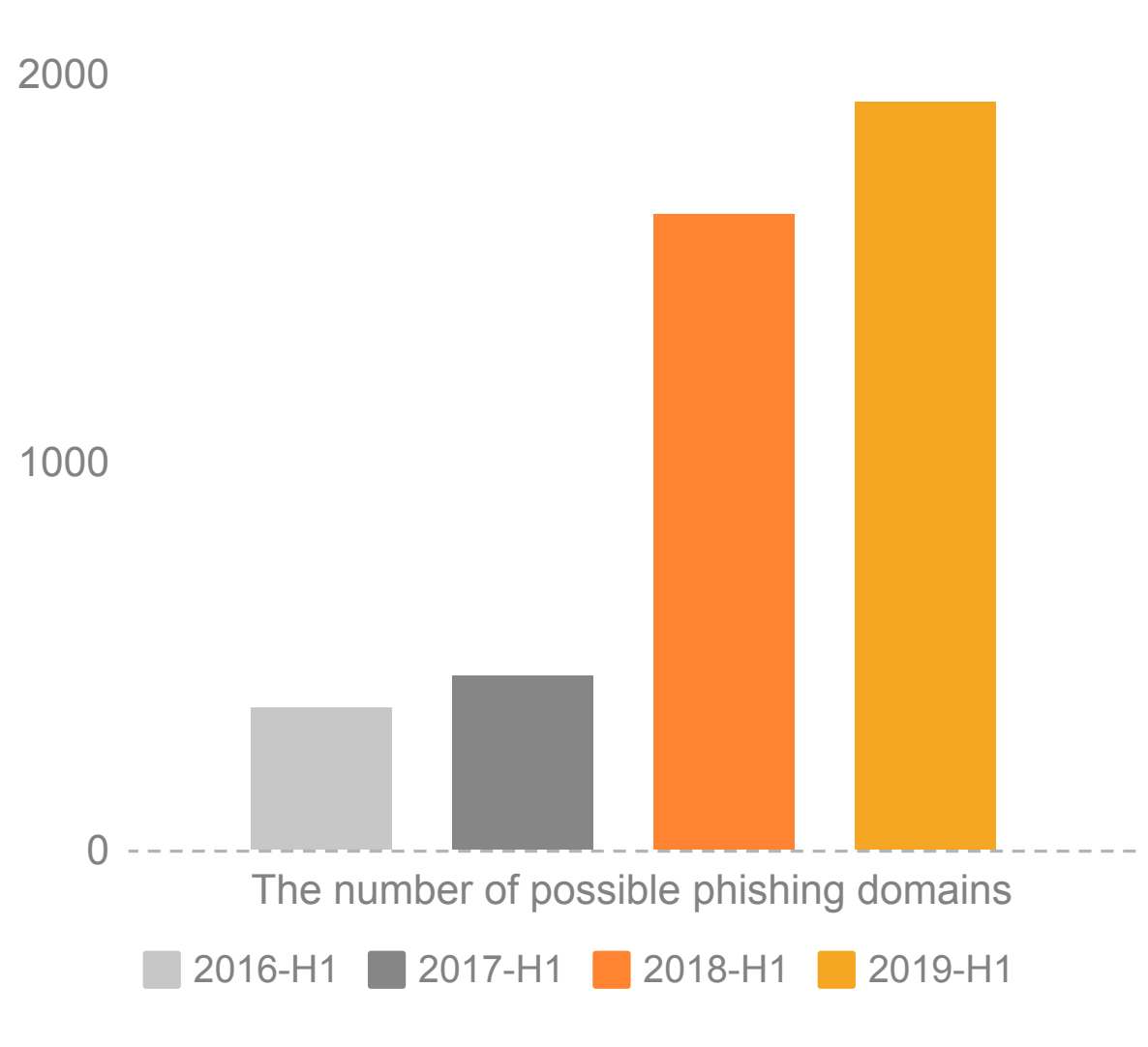
Geographical distribution of the banks studied



Geographical distribution of the phishing domains for the studied banks

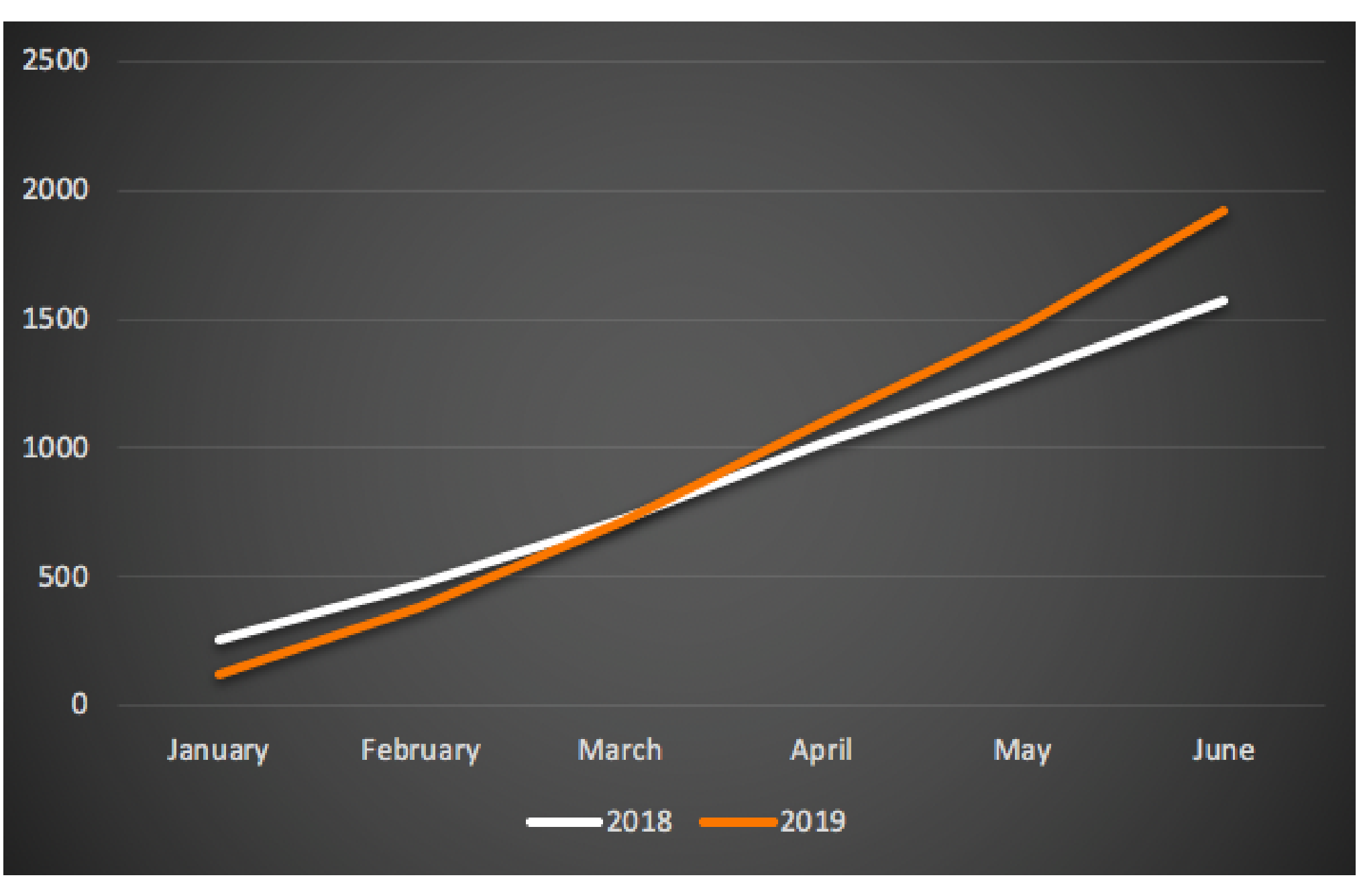
Banks in America are more at risk.

**Although cybercrime covers a wide remit of offenses perpetrated online, it is phishing that is a primary concern for financial institutions. There was a 14% increase in the number of phishing domains registered in the first half of 2019 compared to the ones registered in the same period in 2018.**



## Phishing domains are on the rise

Number of potential phishing domains registered in the year



*Cumulative number of potential phishing domains registered.*

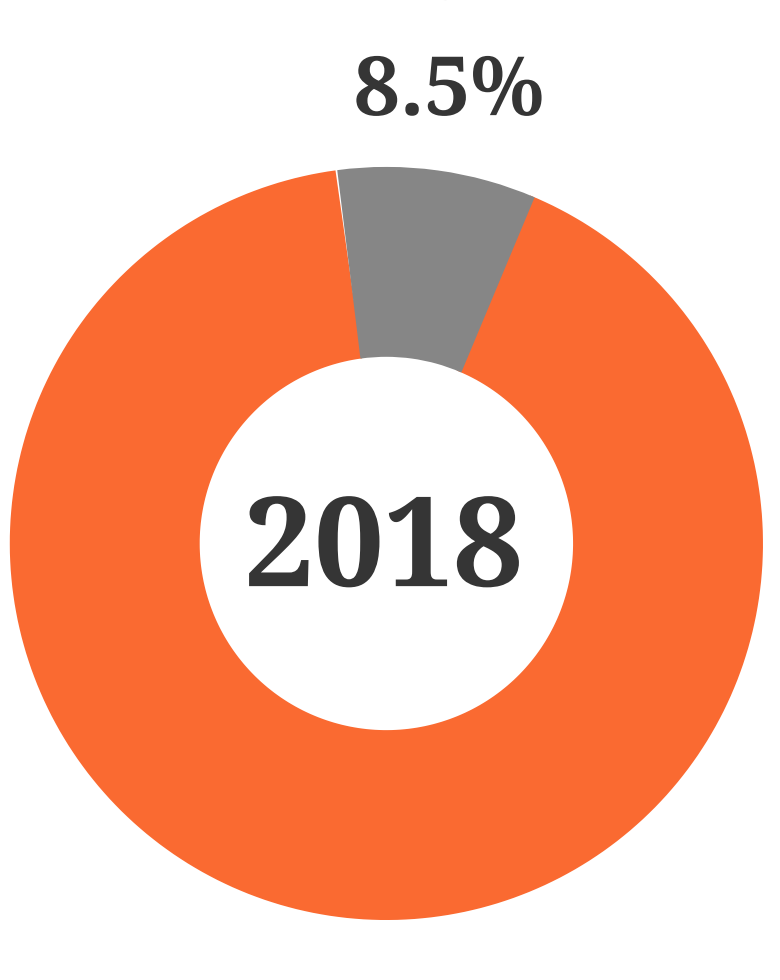
01 **Slow Start-Rapid Increase**
In 2019, potential phishing domains started to appear very slowly, but rapidly increased after March.

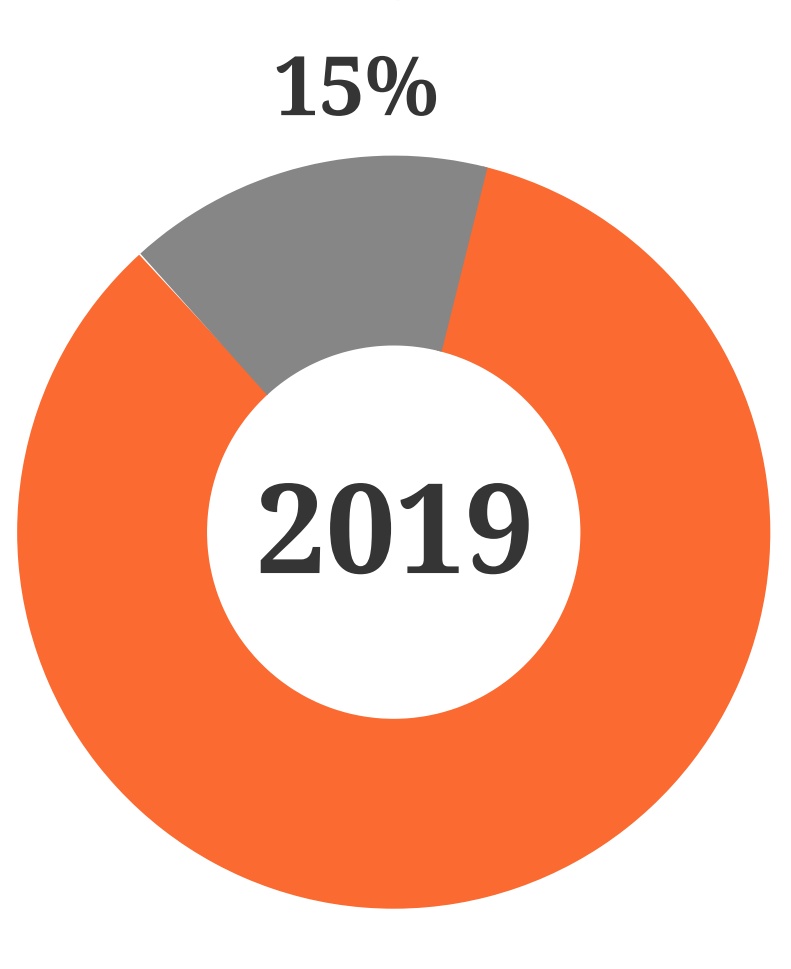
02 **Expected to exceed 3,500**
The projections for the last 6 months of 2019 indicates that the number of potential phishing domains may exceed 3,500.

03 **Some domains are still a risk**
Instead of beginning the scam immediately, hackers may wait for the right moment. So domains that were registered in the 2018 are still at risk.

## Certified Phishing Domain

has a valid certificate

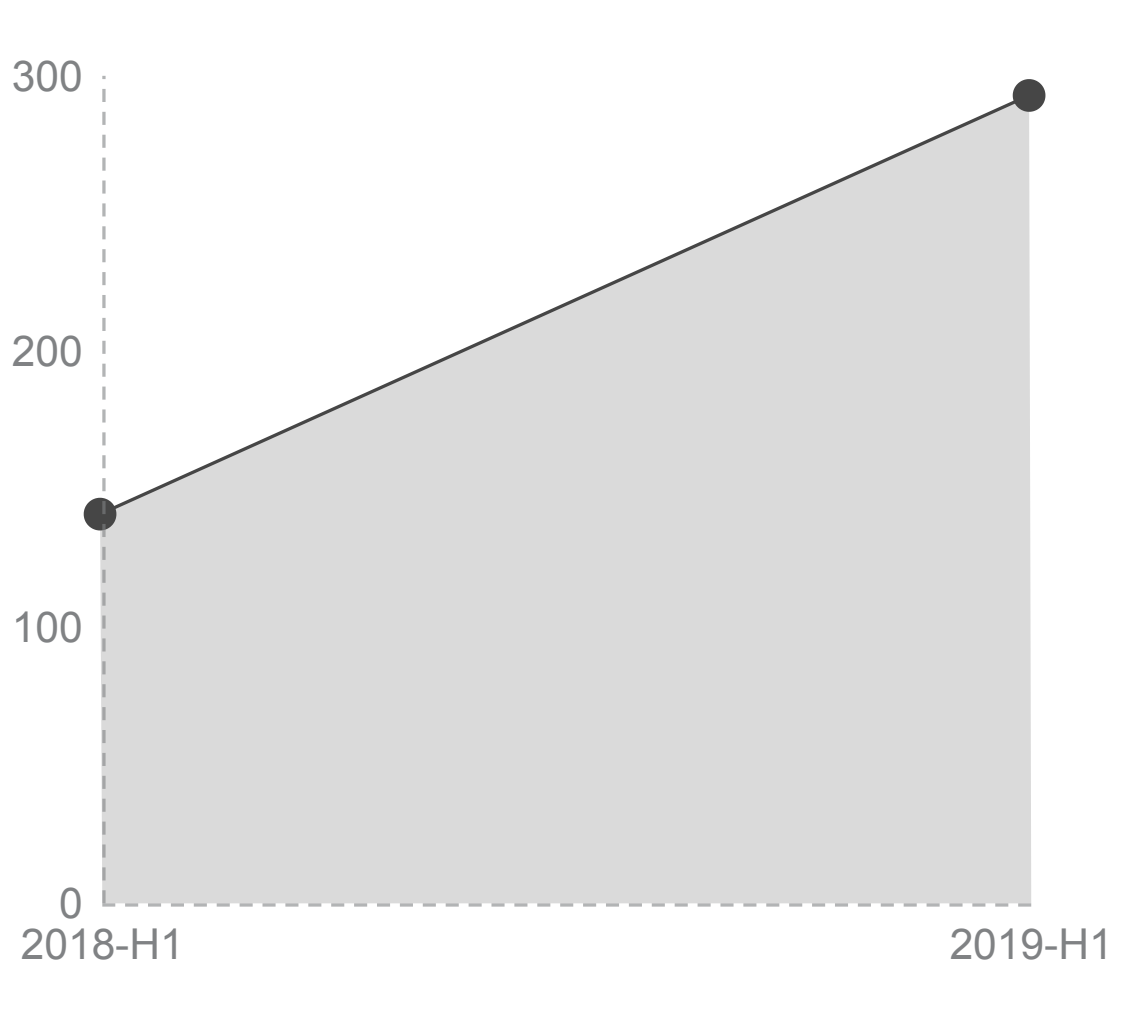




**The padlock icon (🔒) at the browser's address bar (https at the URL) indicates that a domain has a valid SSL or TLS certificate and a certain level of security. However, 15% of potential phishing domains registered in H1 of 2019 impersonated banks having valid certificates.**

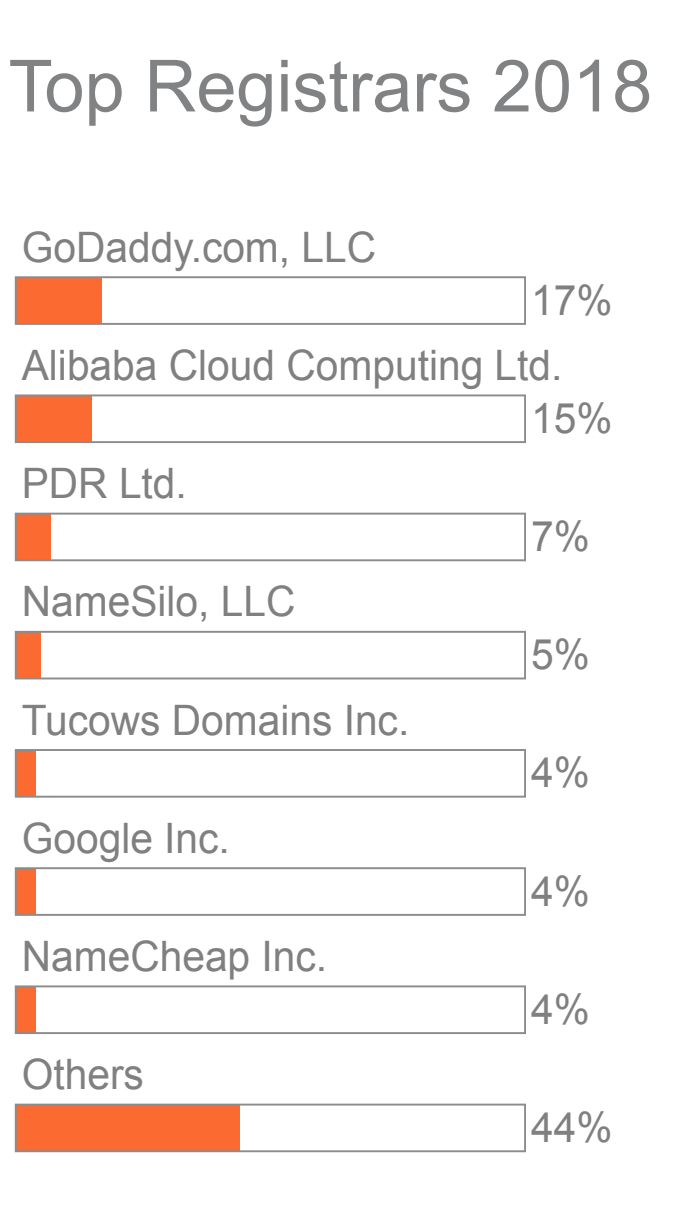
**The number of certified phishing domains increased more than 2X as compared to 2018-H1.**

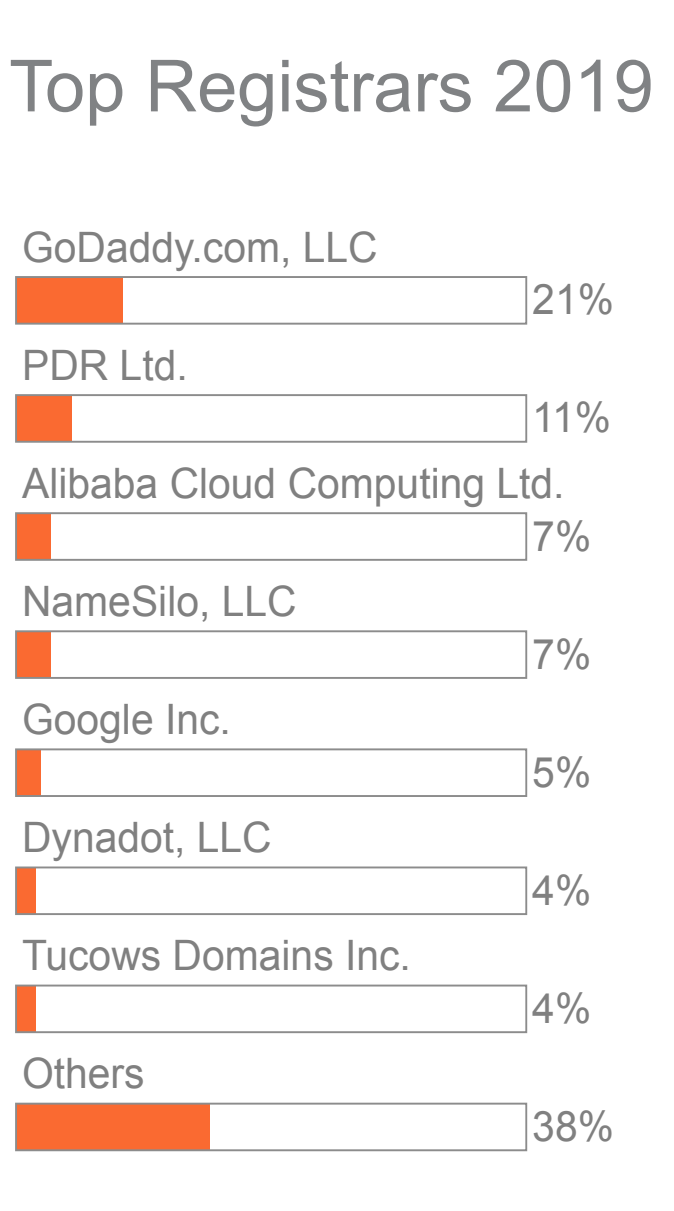
**Every year, hackers improve their techniques and become more intelligent. It is no surprise to see the increase in the number of phishing domains with valid certificates.**



## Top Registarars

**The potential phishing domains are mostly registered by well-known and widely-used registrars such as GoDaddy.**





## Phishing Domain Facts

**Loss of reputation** Phishing domains are exploited to target not only employees but also customers. Even though companies cannot be directly held responsible for customers deceived by phishing scams, it is a loss of reputation when a company does not take precautionary measures.

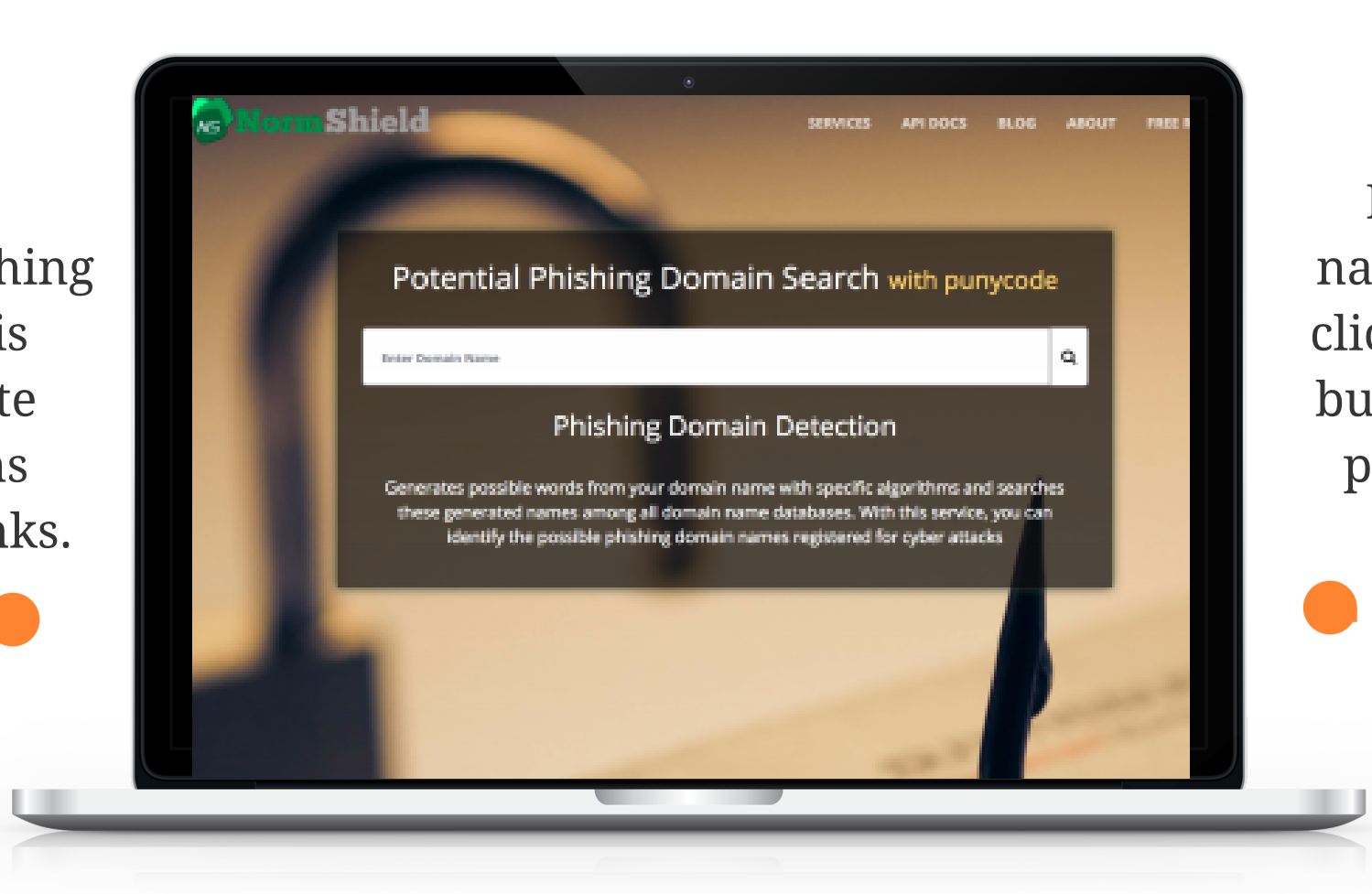
**Data Breach** In recent events, the number of breaches caused by phished credentials is more than breaches caused by other reasons such as malware and unpatched systems combined.

**Cover Tracks** Name-blending phishing domains are exploited not only for phishing attacks to steal credentials but also for attackers to cover their tracks in malicious code.

**Monitor** It is very difficult for a company to search the entire web and uncover a phishing domain that may target its employees and customers. There are certain tools that can be used for this purpose such as NormShield's Free Phishing Domain Search.

## Phishing Domain Search

NormShield's Free 'Potential Phishing Domain Search' is used to investigate phishing domains impersonating banks.



Potential Phishing Domain Search with punycode

Phishing Domain Detection

Generates possible words from your domain name with specific algorithms and searches these generated names among all domain name databases. With this service, you can identify the possible phishing domain names registered for cyber attacks

Enter domain name, hit enter or click on the search button. Use of this powerful tool is quite easy.

NormShield's Phishing Domain Search generates word combinations for the given domain name with specific algorithms and searches these generated names among all the domain name databases. With this service, you can identify potential phishing domain names registered for cyber attacks.

https://services.normshield.com/phishing-domain-search

## Search Tips

### Examine the result

The results are potential phishing domains. Phishing domains are created with missing letters, letter-swapping, and many other techniques.

### Avoid 2- or 3-letter domain names

2- or 3-letter domain names (such as www.db.com) creates too many false positives. Because, there are too many derivatives that are actually legitimate sites. It is better to search for longer versions of those domains like deutschebank.com.

### Avoid generic domain names

Some bank domain names have broad meanings and may create false positives. Instead search for longer versions.

### Check the creation date

The creation date of a website is a good hint to understand on which potential phishing domains to focus. Check the newly created ones first.

DETERMINE - ASSESS- MANAGE

## ABOUT US

Trusted Security Rating Service

**NormShield, trusted security rating services, provides Cyber Risk Scorecards for companies across many categories. NormShield Cyber Risk Scorecards provide the information necessary to protect businesses from cyber-attacks including phishing domains.**

**Do you know where your vulnerabilities lie? Not all risks are foreseeable. Today, threats are unpredictable, both internal and external, and securing the walls of your organization is, simply just not enough. How can you defend your organization and make it more secure? Learn more...**

## LET'S GET IN TOUCH

www.normshield.com/

info@normshield.com

8609 Westwood Center Dr.
Ste 110, Vienna, VA 22182

+1 (571) 335-0222

@normshield

/company/normshield

https://www.normshield.com/