2018 Airlines Phishing Report

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

Welcome to

2018 Airlines Phishing Report

Phishing domains impersonating legitimate websites increase cyber risk.

As the holiday season arrives, many buy airline tickets to travel to their loved ones or to relax in a nice place. Hackers are eager to exploit this urge of people by creating websites (phishing domains) of major airlines to steal personal and payment information. This report reveals how many potential phishing domains are registered just in 2018.

EXECUTIVE SUMMARY

50

Major airlines

all around the world studied in this research.

1,300+

Potential phishing domains

are registered in 2018 so far and expected to exceed 1,600 at the end of the year.

15%

reduction compared to 2017

but caused more damage.

x2

Certified potential phishing domains

registered compared to ones registered in 2017.

Contents

We provide the report in six easy-to-follow sections to grasp the findings.

Airlines hit by serious cyber attacks caused significant data breach in the last four years.

In 2015, major cyber attacks to airlines were only motivated for reward points. The motivation altered to passenger information in 2016 and 2017. However, it has evolved to passenger information and credit card information in 2018. In some attacks, **phishing-domain use was part of the scam,** as in 2018 British Airways data breach where 380,000 customer payment information was stolen.

1st GENERATION

Goal: Reward points

In 2015, customer loyalty program accounts of United & American Airlines compromised and misused.
Same year, British Airways customer frequent flyer accounts compromised.

2nd GENERATION

Goal: Personal info

In 2016 and 2017, the personal data of various airlines' customers were breached. Stolen data included names, passport numbers, travel information, etc.

3rd GENERATION

Goal: Payment info

In 2018 attacks to Cathay Pacific and British Airways, besides personal data, customer credit card details were also breached.

Potential phishing domains for 50 Major airlines all around the world are studied.

We search for potential phishing domains for major airlines with **NormShield's Free Phishing Domain Search** (https://services.normshield.com/phishing-domain-search)*

SEARCH TIPS

✓ Examine the results

The results are potential phishing domains. Phishing domains are created with missing letters, letter-swapping, and many other techniques.
(www.sing**a**poreairlines.com -> www.sin**q**aporeairlines.com)

✓ Avoid 2- or 3-letter domain names

2-letter domain names (such as www.aa.com) creates too many false positives. Because, there are too many derivatives that are actually legitimate sites. That is also valid for 3-letter domain names (klm, jal, ana, tc.). It is better to search for longer version of those domains like americanairlines.com

✓ Avoid generic domain names

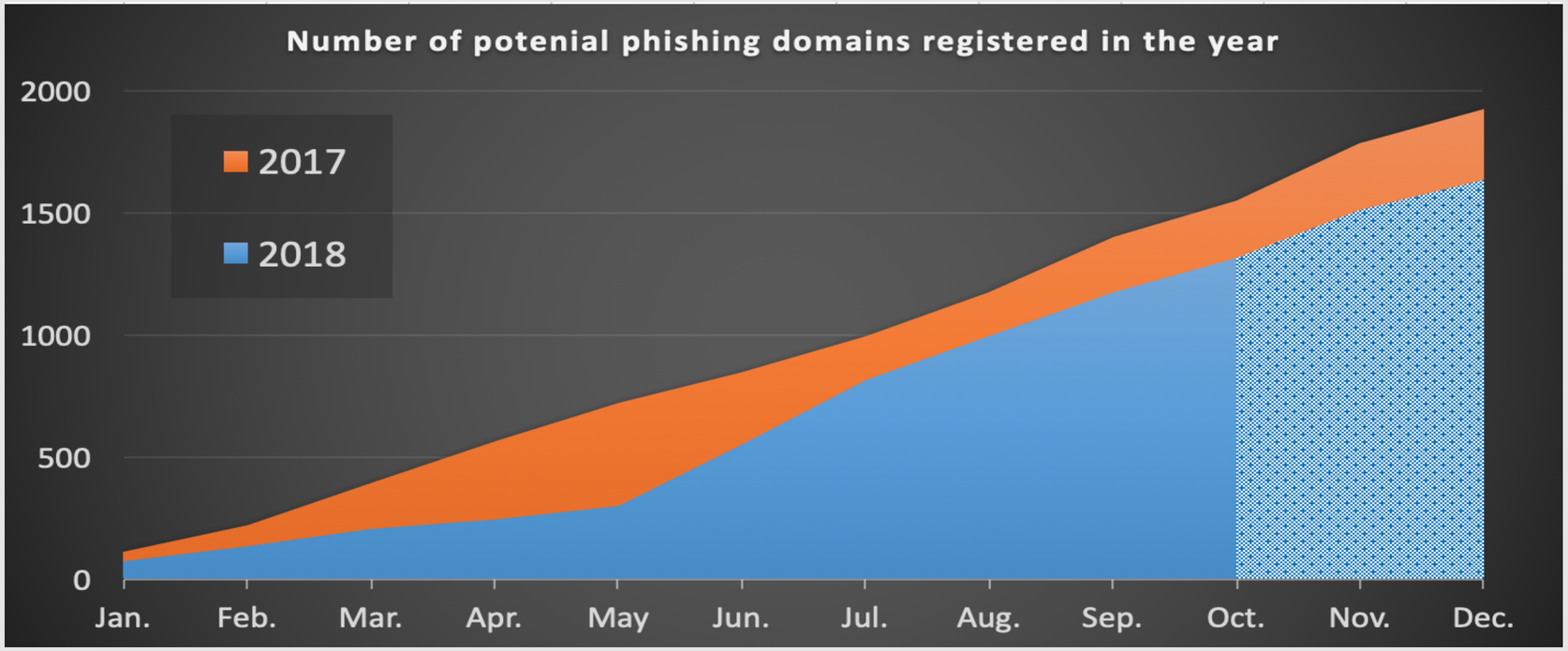
Some airline domain names such as swiss.com, austian.com, etc. have broad meanings and may create false positives. Instead search for longer versions such as swissair.com, austrianairlines.at, etc.

✓ 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 new ones first. Without creation-date limitation, there are more than 11,000 potential phishing domains for these airlines.

* To learn more about how to search potential phishing domains with NormShield's Phishing Domain Search click here.

There are more than 1,300 phishing domains registered in the first 10 months of 2018.



Cumulative number of potential phishing domains registered.

01

15% Reduction

The number of phishing domains registered in the first 10 months of 2018 are 15% less than the ones in the same duration of 2017.

02

Slow start - Rapid increase

In 2018, the potential phishing domains started to appear very slowly, but rapidly increased after May, especially due to holiday season.

03

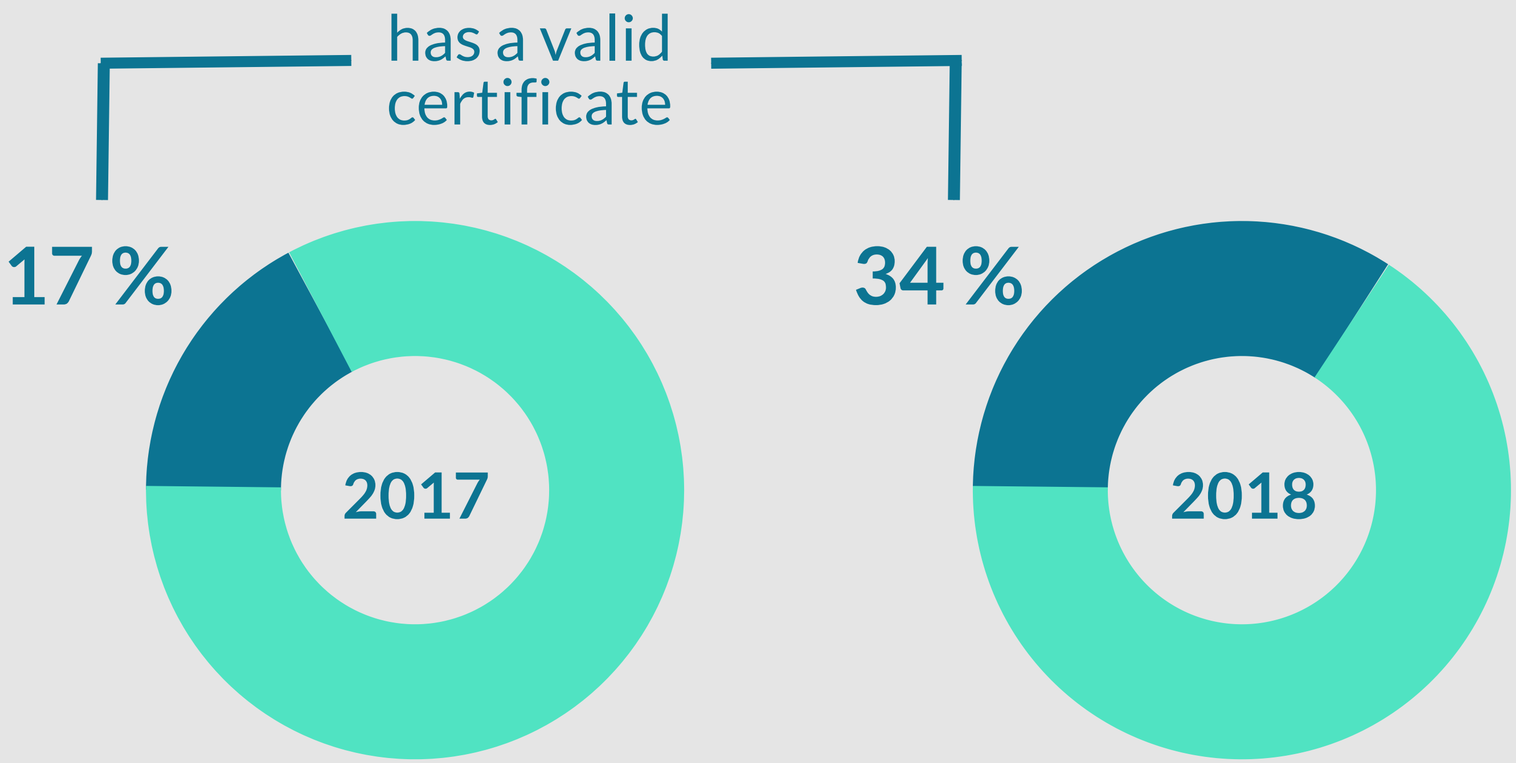
Expected to exceed 1,600

The projections of increase for the last 2 months of 2018 indicates that the number of potential phishing domains may exceed 1,600 (still lower than 2017)

04

Some of the domains from 2017 is still a risk

Some hackers register a phishing domain, but not necessarily start the scam right away. They may want to wait for some time. Hence, some of the domains registered in 2017 still pose a risk.



Hackers try to gain trust by getting valid certificates for their phishing domains.

https://

FINDING #1

34% of domains has a certificate

The padlock icon (https at the URL) indicates that a domain has a valid SSL or TLS certificate and a certain level of security. However, 34% of potential phishing domains also has a valid certificate.

x2

FINDING #2

Certified domains doubled

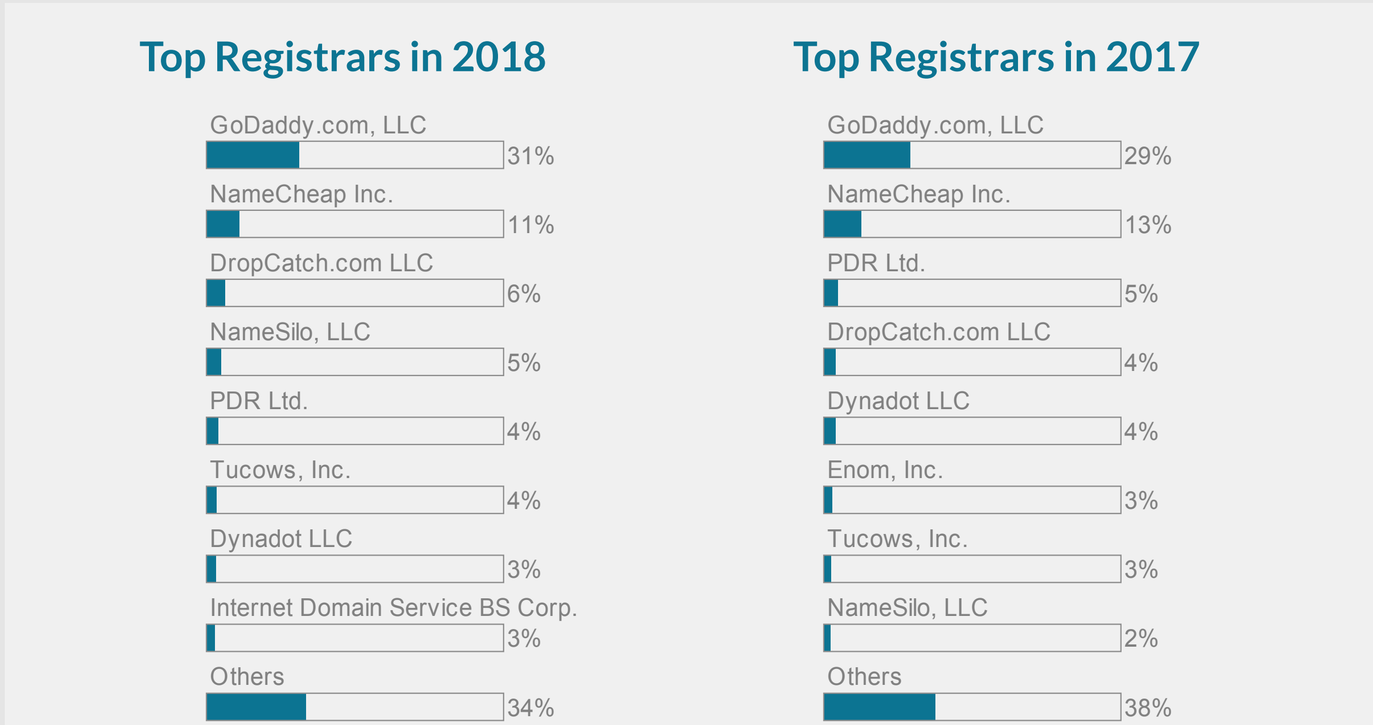
The ratio of potential phishing domains with a valid certificate doubled in 2018 compared to last year.

FINDING #3

Techniques are evolved

Every year, hackers improve their techniques and become more clever. That's why It is no surprise to see the increase in the number of phishing domains with a valid certificate.

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



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 necessary measures.

✓ One of the major cause of data breach

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

✓ Can be used to cover tracks

Name-blending phishing domains are exploited not only for phishing attacks to steal credential s but also for attackers to cover their tracks in malicious codes. For the recent advanced attacks against British Airways and Newegg, hackers inserted phishing domains into malicious codes to cover their tracks.

✓ How to monitor

It is very difficult for a company to search entire web and determine a phishing domain that may target its employees and customers, but there are certain tools that can be used for those purposes such as NormShield's Free Phishing Domain Search.

NormShield
TRUSTED SECURITY RATING SERVICES

EVALUATE. REMEDIATE. VERIFY.

Cyber Risk Scorecards

NormShield, trusted security rating services, provides Cyber Risk Scorecard for companies with many categories. NormShield Cyber Risk Scorecards provide the information necessary to protect business from cyber-attacks including phishing domains. The scorecards provide a letter grade and a drill down into the data for each risk category so that remediation of vulnerabilities can be prioritized.

LEARN MORE

NormShield

TRUSTED SECURITY RATING SERVICES

Know what hackers already know about you.

Knowing your Cyber Risk Score equips you with the information necessary to protect your business from cyber attacks and it increases your awareness against third party risks. NormShield Cyber Risk Scorecards allow you to monitor your own cyber risks as well as the cyber hygiene of your entire vendor ecosystem. With easy-to-understand letter-grade scores, you will have a clear view of your security posture.

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