NormShield

THE STATE OF FINANCIAL PHISHING 2019 H1

Cyber criminals continue to use phishing to lure bank customers and steal personal and financial information. Where and how have phishers attacked in 2019?

Phishing attacks always start with a scheme to trick consumers into thinking they are doing business with a company or organization that they already trust. Hackers create websites that impersonate financial institutions and then steal sensitive information such as credit card and banking data that consumers openly share.

Phishing attacks are extremely costly for consumers and banks – both monetarily and reputationally. A phishing attack greatly damages trust and brand reputations.

Phishing At a Glance

Increase over H1 2018

50 major banks
NormShield investigated 50 major global financial institutions

1,900+
Potential phishing domains registered in the first half of 2019

14%
Increase in potential phishing domains

2X
Double the potential phishing domains that were certified by registrars

Phishing in Action

Phishing attacks are more complex and targeted.

Cyber criminals are capable of mimicking actual promotions being run by financial institutions and produce convincing scenarios that are able to easily fool even the most cyber-aware consumers.

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

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

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

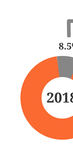
August - 2018
Phishing emails imitated various messages from major Turkish banks

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

Phishing At a Global Scale

The number of potential phishing domains for European banks is higher than the ones in any region.

Geographical distribution of the potential phishing domains for the studied banks



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

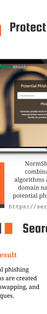
01
Slow Start-Rapid Increase
In 2019, potential phishing domains started to appear very slowly, but rapidly increased after March.

02
3.5K+
By year's end, more than 3,500 new phishing domains will be active.

03
Attacks in Waiting
Hackers like to wait for the right moment. Some domains that were registered last year, but not used, are still at risk for activation.

The Padlock Can Lie

Potential Phishing Domains with 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 domains that can potentially be used for phishing 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 potential phishing domains with valid certificates.

Top Registrars

Phishers use a wide variety of registrars to purchase domains.

Top Registrars 2018

Top Registrars 2019

The Impact

Loss of reputation
Phishing domains target bank employees and customers. Even though companies cannot be directly held responsible for customers' deceived by phishing scams, it is a significant hit to brand reputation and customer trust.

Data Breech
Phishing is the number one cause of data breaches.

More Attacks
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.

Protect Yourself

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

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.