Sur.ly Blog

How To Identify And Neutralize Phishing Attacks

BY SUR.LY TEAM ON SEPTEMBER 22, 2017 | NEWS AND ANALYTICS

Everyone who often deals with the Web has ever heard the term 'phishing attack'. Today we will explain what a phishing attack is, reveal its mechanisms, and give you effective tips on how to recognize and rebuff any phishing attempts.

What is phishing attack and where may it come from?

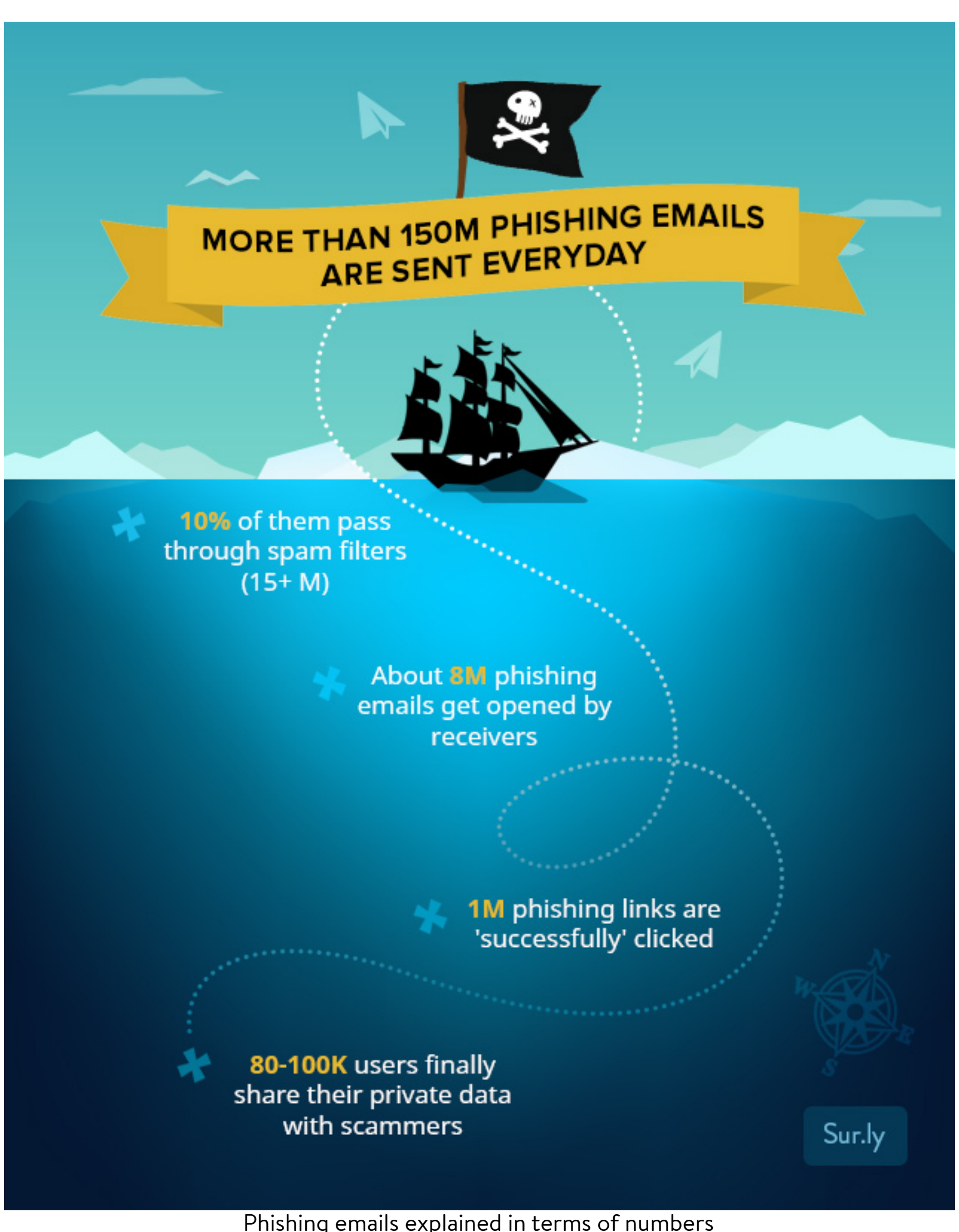
Wiki gives an absolutely clear-cut phishing attack definition:

> *"Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication".*

We at Sur.ly would like to add that the phishing methods are evolving all the time adopting new ways of a fraud, so it's nearly impossible to define and prevent all types of phishing attacks, but they basically include the following:

- **Fake emails** (or sometimes instant messages) with dangerous links or attachments. Hackers can easily spoof brand styles, logos, etc.
- **Dummy web forms** imitating trusted forms, such as payment service forms, login pages or account recovery forms.
- **Domain name system (DNS) poisoning** – it includes a web browser hijacking program that replaces a legit URL with a rogue address.

Be aware, be secure: phishing messages or forms may look very realistic and legitimate these days, and they can come from sources/people you closely know or trust (as their email accounts might get accidentally hijacked).



Phishing emails explained in terms of numbers

Large-scale phishing attacks were recently reported: particularly, some of them exploited critical Gmail's vulnerabilities, such as one of the biggest scam campaigns which targeted at least a million of private and corporate Gmail users – it was a sophisticated 'full cycle' spam attack, including fake but realistic emails, spreading malicious links via infected users' mail lists (and thus technically coming to potential victims from their friends or coworkers), and asking to grant a permission to a hacker application imitating Google Docs to check some important document, but actually taking user accounts under control.

Other attackers can be also trying to intrude to your system through the vulnerabilities of Microsoft Office: you may get an email with a document attachment that when opened will trigger a remote malware download via MS Word, resulting in infection on your system. These two phishing attack types are quite different, but their end goal is common: take your private data under control, so unknown hackers can steal it (e.g. bank account credentials, email logins, security codes, etc).

How to identify phishing attack: 5 common indicators of a phishing email

Even if you don't have some special IT-wise knowledge, you can use these simple criteria to identify the phishing attack emails:

1. Basic-level phishing stuff **doesn't use personalized salutations** (such as addressing a user by their first and last name), but it rather starts with common greetings like '*Hello dear customer!*' Also, it may lack a legit company's official signature or other important details.
2. Most of legitimate, trustworthy organizations **will never contact clients or customers** asking them to enter private credentials or other secret information by clicking on a link to a website.
3. Phishing emails are usually trying to **create a sense of urgency**, convincing you of necessity to follow the links, for example, to re-enter/confirm your credentials, telling that if you don't act immediately, you'll lose access to your account, etc.
4. **Check it for spelling mistakes**: normally, brands are very serious about grammar in their official communications, so if you can spot a mistake, then most likely it's a fraud.
5. **Check the domain it came from**: if a sender's email address looks spoof or weird, disregard and delete the unsolicited email immediately (the same way you can check links, if it contains any – just hover your mouse over them, but don't click).

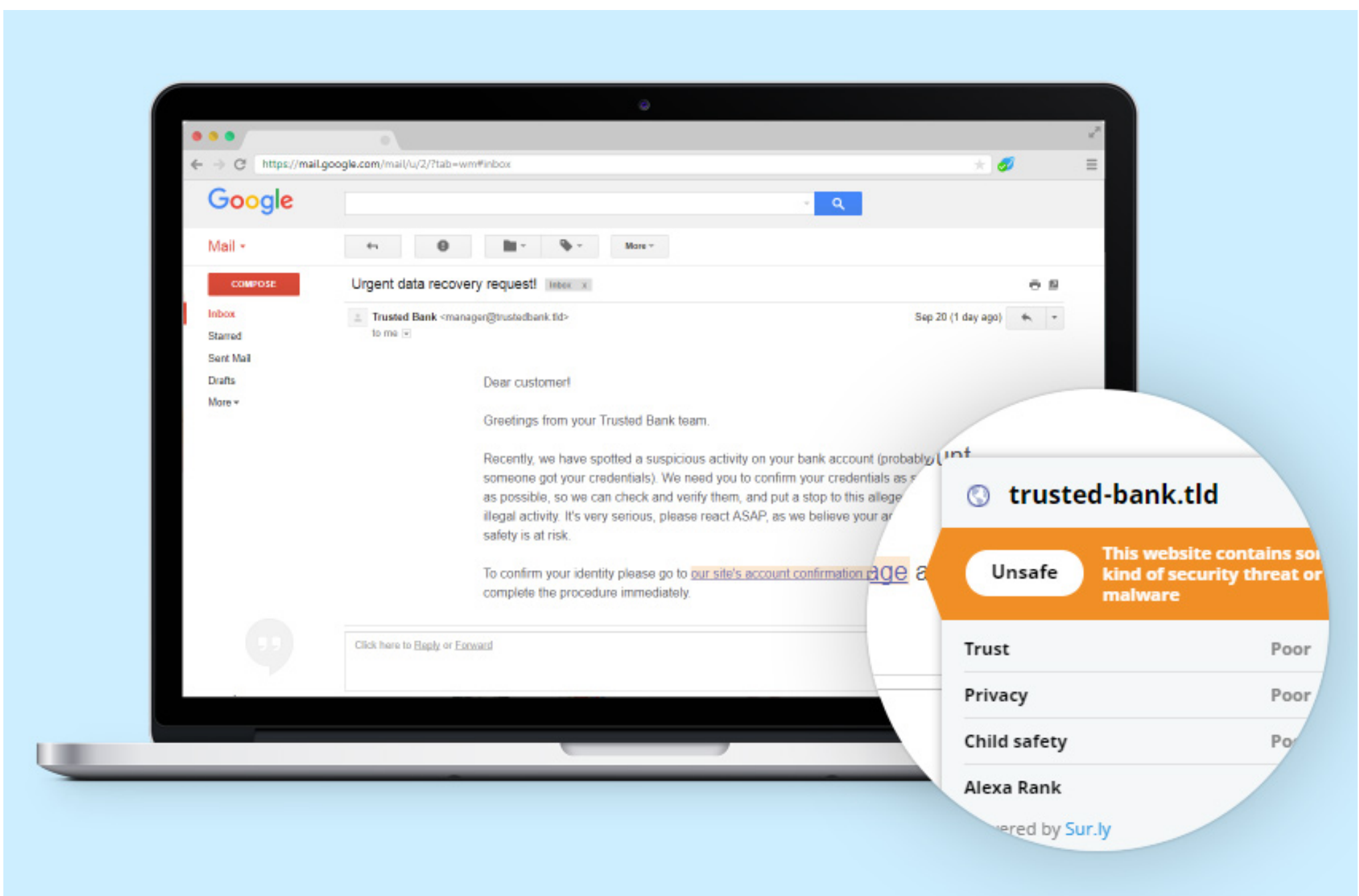
What can hackers do with your data? Actually, they have a bunch of options!

How can you make sure you will not fall victim to a phishing attack?

There are still too many vulnerabilities in all powerful software that we use on daily basis (including the system itself and third-party packages of all sorts) so the phishing attempts will continue, giving hackers uncountable chances to break through our firewalls and steal our data.

However, there are a few more simple tips that won't let you fall victim to all kinds of phishing tricks:

- **The golden rule is**: Never click on a link or attachment in a message or email that you're not expecting, or until you're completely sure it's not fake. If a letter comes from a person you know, it's better to message or call him/her personally to confirm it's legit (the same is true for organizations: better call their hotline and get their official confirmation that the letter is not fake).
- **Always check a link before clicking on it**: You can always hover your mouse over a link within a letter to preview an address which it really leads to, usually in the left bottom corner of a browser window (however, hackers can spoof even this one, so a phishing link may show a legitimate address when you hover your mouse over it).
- **Find additional software** which would help you preview safety status of a link before clicking on it. Such as Sur.ly Surfguard – a free web browser extension that allows checking a status of any link (whether it's in Google's search results, on a page, or in a letter) just by hovering over them (see the picture) – it highlights all suspicious or adult links and provides you with additional info.



Sur.ly Surfguard shows malware notification when you hover the mouse over a link

Surfguard extension is connected to our own evergrowing and constantly updated database of website statuses (based on user reports and data from popular web reputation systems) that supplies it with a pretty accurate verdict on whether a certain site is a scam or dangerous for a reason, so you can easily check links without opening them.

Recent posts

How To Keep Visitors On Your Website Longer?

POSTED ON SEPTEMBER 14, 2017

It comes as no surprise that every website owner who worked day and night to build his/her project is always in search of 'holy grail' trying to invent a better way to retain visitors, get people interested, focused on the site's content, and then straightforwardly converted into sales or sale leads.

Sur.ly Surfguard is here!

POSTED ON SEPTEMBER 1, 2017

Sur.ly Surfguard is here! It's a browser addition powered by our web safety platform, which lets you preview status of a link before clicking on it. If a link is unsafe, you'll get a pop-up notification when hovering your mouse over it.

I am not a robot: How to stop human-generated fake user registrations on any platform

POSTED ON AUGUST 22, 2017

If you run a free membership site of any kind, then you surely have a first-hand experience of dealing with spam signups. Such fake registrations are a pure garbage that adds no value to your user base, ruins the overall picture of your audience, and can do no good to any marketing efforts: the more […]

Sur.ly News

- Sur.ly Surfguard is here! It's a browser addition powered by our web safety platform, which lets you preview status of a link before clicking on it. If a link is unsafe, you'll get a pop-up notification when hovering your mouse over it. — 01 September 2017
- Meet the Sur.ly blog! A place where we'd be happy to share our expertise, useful tips, analytics, and best insights into the world of SEO, link building and spam-fighting. — 16 August 2017
- Updated FAQ section: up-to-date answers and instructions are ready to guide you on Sur.ly's features and best practices. — 05 May 2017