SAFEDNS

As cybercrime statistics of recent years state, 71% of hacker groups that committed attacks from 2017-2020 used targeted email phishing (according to Symantec), making it one of the most popular hacking methods among attackers.

Phishing is the most common way to deceive a user. During the attack, attackers try to pass themselves off as someone a person trusts: they send phishing emails, fraudulent text messages, messages in messengers and social networks, create fake sites on the Internet, etc.

To effectively distinguish between phishing links and emails, you first need to understand domain levels:

1 level domain is:
cool.mail.safedns.com, etc.

2 level domain is:
cool.mail.safedns.com, etc.

3 level domain is:
cool.mail.safedns.com, etc.

4 level domain is:
cool.mail.safedns.com, etc.

The important thing to understand is:

To create a third-level domain (for example, **mail**.safedns.com) you need to be the owner of the second-level domain – **safedns**.com. There is no chance that a second-level domain belongs to one owner, but a third-level domain to another one.

So if you see the address mail.safedns.com and newmail.safedns.com (instead of SafeDNS domain you should use your company's one), you can be sure that both addresses belong to the domain safedns.com and as a consequence,

to the company SafeDNS.

But if you see addresses like mail.**safedns**.com & mail.**safe-dns**.com, stay aware: these are two completely different second-level domains and you should verify that mail.safe-dns.com belongs to SafeDNS.

Contacts

+ 1 800.820.2530 (US)
+ 1 571.421.2990 (Outside US)

sales@safedns.com
safedns.com

Signs an email contains phishing:

Signatures

Often phishing emails are signed with the name of the department, not referring to a specific employee of the company (e.g., Regards, Information Security Department)

Unknown domain address

For example, our company's mail server domain is @safedns.com.

An employee's email address would be john@safedns.com.

Scammers change the domain name slightly, such as john@safe-dns.com or john@safedns.info, counting on the attention of employees.

Second level domain spoofing

You get an email saying that your password has been cracked and you urgently need to click on a link to change it.

If you hover your cursor over the link (without clicking!), you will see the address where the link actually leads in your browser at the bottom left. If the real address of the company looks like this: safedns.com/, then the phishing link would be something like: safe.dns.com/, safedns.something.com/ or safe-dns.com, etc.

Urgency

t's important for scammers to not let you even start thinking. To avoid it, they often use urgency-related words, such as “send asap”, “I am waiting”, “please send now” etc.

Password change

If your email asks you to change your password, but when you click on the link you are prompted to log in first, it's worth carefully checking the url of the page for spoofing. For example, in our company our corporate mail is at mail.safedns.com, but you have to log in at mail.safe-dns.com - this is not okay.

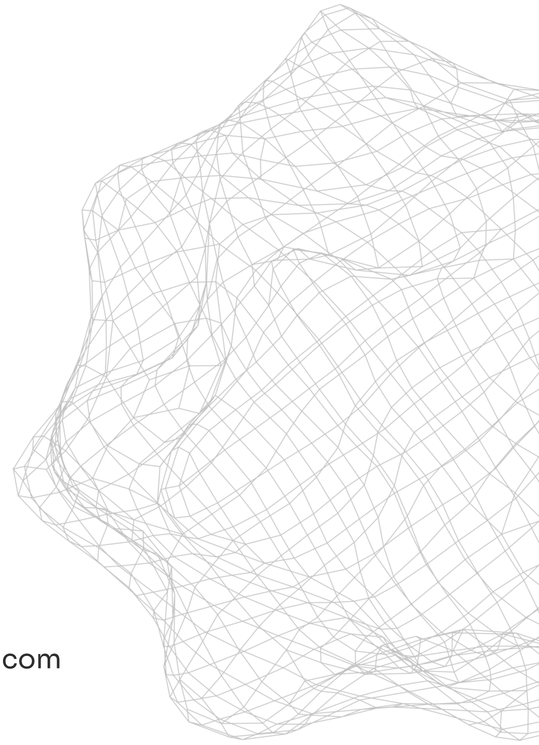
Spelling mistakes

To bypass spam filters, scammers purposely change the words or make mistakes in emails.

Examples are "sendpassword" or "send pasword", etc.

Non-personal appeals

Universal, non-personal appeals, such as "Dear Employees," etc.



Contacts

+ 1 800.820.2530 (US)
+ 1 571.421.2990 (Outside US)

sales@safedns.com
safedns.com

SAFEDNS

What NOT to do if I receive a phishing email?

- Click on links from emails that you weren't expecting, that are suspicious, or that were received from addresses not from your contact list
- Open attachments in emails that seem suspicious to you - often attackers disguise viruses as ordinary office files such as .docx, .pdf, etc
- Send confidential company data in response to an email you receive
- Give access to a company service (Jira, Slack, Gitlab, etc.)
- Disclose your personal information in a reply email or on the attacker's site
- Disclose other employees' personal information in a reply email or on the attacker's website
- Forward the phishing email to other company employees
- Distribute URLs or attachments obtained from phishing emails within the company.

What should I Do if I get a suspicious email?

- Do not click on links in the email, open attachments or send passwords and confidential data of yourself and the company.
- If there is a specific person or department named in the signature of the email, contact them and see if they sent the email.
- If the mail is not from a specified department or employee, report the email to the technical support department.
- Alert your colleagues in private chats about a phishing attack on the company. Move the email to spam.

Contacts

+ 1 800.820.2530 (US)
+ 1 571.421.2990 (Outside US)

sales@safedns.com
safedns.com