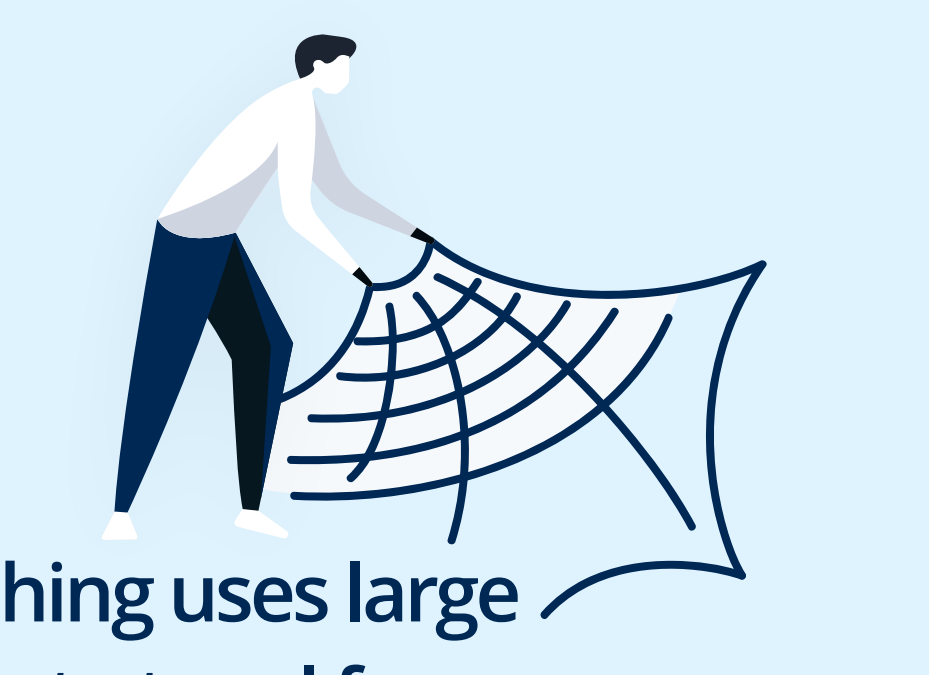
How to Spot a (Spear) Phisher

Spear-phishing is a more targeted and dangerous form of phishing.

Did You Know?

According to Proofpoint's State of the Phish report, 79% of businesses experienced targeted (spear phishing) attacks in 2021 – a 20% increase from 2020. Moreover, 94% of these highly targeted emails utilize malicious file attachments as the starting point of the infection.



Phishing uses large nets to trawl for a maximum amount of random victims.

Spear-phishing uses a sharp, targeted spear to go after a big prize.

Phishing	Applies to both	Spear-phishing
High-volume: spammed to hundreds or thousands of people.	Coercive language or a sense of urgency will motivate the target to act.	Low-volume: send to one person or a small group of people, like the finance department.
Non-personalized: generic greetings, etc.	Delivered via email.	Highly personalized: attackers will research their targets in order to craft an email that's believable.
Generally delivered via malicious links or attachmets.	Hackers are after login credentials, sensitive information, or money.	Zero-playload attackes are common.
	Rely on impersonation	

History's Most Notable Spear-Phishing Attacks

2021

- NOBELLIUM, the hacking group responsible for the SolarWinds breach, launched spear-phishing campaigns against US government agencies under the guise of 'election fraud documents'.
- Scammers hit UK rail network Merseyrail with a Lockbit ransomware attack through spear-phishing emails sent to employees.
- Russian hacking group Gamaredon (aka ACTINIUM) has been sending spear-phishing emails against Ukrainian gov't and NGOs since October 2021.

2020

- Staff from social media giant Twitter were spear-phished into giving account credentials that allowed hackers access to celebrity accounts and enabled them to steal $100,000 worth of Bitcoin from their followers.

2016

- Belgian bank Crelan lost €70M from spear-phishing attacks and organized fraud.
- Austrian aerospace parts maker FACC fires the CEO after a €42M spear-phishing attack.

2015

- Evaldas Rimasauskas, a Lithuanian national, stole $100M from two of the biggest tech giants, Google and Facebook through spear-phishing emails targeted at their employees.

An example of a spear-phishing email (and how to spot the spoofs)

A false sense of urgency. Remember: If you see an "urgent" email, be alert. No reputable person or company will ask to sacrifice security for speed.

Subject: **Important! Please address IMMEDIATELY**

Jane Smith <jame@companyadc.com>

To: **Matt Peters** <matty@companyabc.com>

Hey, Matty!

I'm at Cambridge, Mass. right now, preparing for my talk tomorrow at MIT (super nervous about it by the way). Just got off the phone with Jessa from ProviderXYZ and she told me we're behind two months on payment for the web dev services??? How embarrassing is that?

Apparently, it was a mixup on their end; we've actually been paying them on an old account from their previous banking provider. Not our fault, but it's still awkward as hell. Could you please wire them the two months worth of payment that we owe? As soon as you can, please, we don't wanna rack up debt.

Details from Jess on the receiving account are here, in a PDF: box.com/s/xx9ftm6pbz855vs9fnwq94rwyqx8b89dkmw

Just email me when it's done, Matty; too busy to talk right now. Counting on you!

Jane

Notice the subtly misspelled email address? Always check every letter of an email address to be sure it's legitimate.

Does this person greet you in emails this way, or do you feel that this is too friendly and that something is off?

Does the email look or sound like anything that the sender has written to you before? If not, this might be a phisher with his spear trained on you.

Another push for urgency here. Again: no reputable person or company will ask to sacrifice security for speed.

Requesting "two months worth of payment" casually, without going through the right channels, should be a red flag.

Always be wary when people are too casual or non-process oriented around anything involving finances or sensitive data.

Avoiding due diligence or avoiding further contact is a tell-tale sign of spear-phishing.

Dangerous outbound links are common than malicious attachments in spear phishing. Never click on links unless you are 100% sure they are safe and come from a trusted sender.

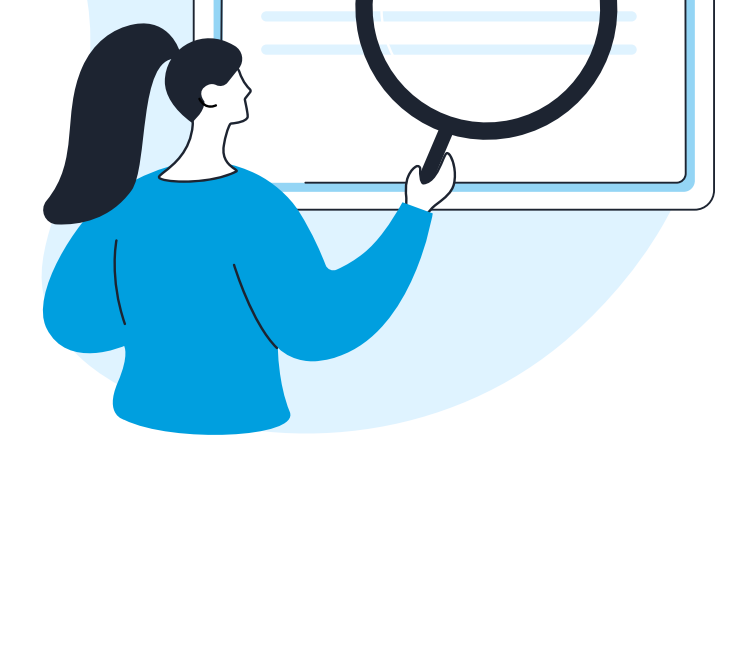
Other ways to verify

Keep calm and call the sender

If the email's demands have the possibility of leading into trouble in the future (like digital espionage or even just plain old theft), do not hesitate to make a phone call to the sender to verify the validity of the email.

Check if the links are spoofed

Hover your cursor over any of the links in the body of the email. If those links don't match the text that appears, chances are, you're talking to a spear-phisher.



Scan the attachments, if there are any

There are some effective antivirus programs that exist online. Try to use those to scan the email's attachments for malicious payloads or obsolete file formats.

Mitigate the risks of spear-phishing. Secure backups and get fully recoverable copies of your systems and information with Dropsuite.

Contact us below:
dropsuite.com
sales@dropsuite.com

Dropsuite