**EUROPOL PUBLISHES LAW ENFORCEMENT AND INDUSTRY REPORT ON SPEAR PHISHING**

*04 November 2019*

*Press Release*

[Print](https://www.europol.europa.eu/print/newsroom/news/europol-publishes-law-enforcement-and-industry-report-spear-phishing)[PDF](https://www.europol.europa.eu/printpdf/newsroom/news/europol-publishes-law-enforcement-and-industry-report-spear-phishing)

* [E-mail](mailto:?subject=Europol%20Publishes%20Law%20Enforcement%20and%20Industry%20Report%20on%20Spear%20Phishing%20%7C%20Europol&body=https%3A%2F%2Fwww.europol.europa.eu%2Fnewsroom%2Fnews%2Feuropol-publishes-law-enforcement-and-industry-report-spear-phishing)
* [Facebook](http://www.facebook.com/share.php?u=https%3A%2F%2Fwww.europol.europa.eu%2Fnewsroom%2Fnews%2Feuropol-publishes-law-enforcement-and-industry-report-spear-phishing&t=Europol%20Publishes%20Law%20Enforcement%20and%20Industry%20Report%20on%20Spear%20Phishing%20%7C%20Europol)
* [Twitter](https://twitter.com/intent/tweet?url=https%3A%2F%2Fwww.europol.europa.eu%2Fnewsroom%2Fnews%2Feuropol-publishes-law-enforcement-and-industry-report-spear-phishing&text=Europol%20Publishes%20Law%20Enforcement%20and%20Industry%20Report%20on%20Spear%20Phishing%20%7C%20Europol)
* [LinkedIn](http://www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fwww.europol.europa.eu%2Fnewsroom%2Fnews%2Feuropol-publishes-law-enforcement-and-industry-report-spear-phishing&title=Europol%20Publishes%20Law%20Enforcement%20and%20Industry%20Report%20on%20Spear%20Phishing%20%7C%20Europol&ro=false&summary=&source=)

THIS NEWS/PRESS RELEASE IS ABOUT [CYBERCRIME](https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime)

[*View all crime areas*](https://www.europol.europa.eu/crime-areas-and-trends/crime-areas)

The Hague

Today, 4 November 2019, Europol’s European Cybercrime Centre ([EC3](https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3)) published a strategic report on spear phishing, reflecting the views of both law enforcement and private industry on one of the most prevalent cyber threats currently affecting organisations across the EU.

Spear phishing describes the practice of targeting specific individuals within an organisation or business for the purposes of distributing malware or extracting sensitive information. As reflected in this year’s Internet Organised Crime Threat Assessment ([IOCTA](https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019)), spear phishing is the number one attack vector and enabler for the vast majority of cybercrimes.

The report is the result of a two-day meeting with the European Cybercrime Centre’s 70 key industry partners from internet security, telecommunications and financial services. The [Joint Advisory Group Meeting](https://www.europol.europa.eu/newsroom/news/europol-teams-industry-experts-to-combat-phishing), which took place on 26 - 27 March 2019, gathered representatives from industry and law enforcement at Europol’s headquarters in The Hague to discuss what can be done to help mitigate this type of crime.

The report highlights the role of spear phishing as the main attack vector for cybercriminals and  contains the definition of the main modi operandi that criminals use to deceive the target (among others, emails coming from trusted accounts, malicious attachments or links to fraudulent websites). Moreover, the document collects conclusions and recommendations for organisations on how to effectively combat this threat on a technical, educational, as well as operational level –enforcing security policies, implementing artificial intelligence and a raising public awareness on the topic.

At the same time, the report highlights some of the challenges related to information-sharing and the investigation of spear phishing attacks. A collaboration effort with law enforcement and the private sector should be done collectively.

Steven Wilson, Head of Europol’s European Cybercrime Centre said: “Spear phishing is a major enabler of some of the most serious forms of cybercrime, especially ransomware, and can cause real harm to European citizens and organisations. We can only tackle a threat of this scale effectively by working closely with key partners from across industry. The [EC3 Advisory Groups](https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners) and this report are a reflection of our ongoing cooperation to tackle the threat from cybercrime.”

Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. EC3’s Advisory Groups on Financial Services, Internet Security and Communication Providers aim at fostering trust and cooperation between key private sector industries and law enforcement in their joint fight against cybercrime. They meet separately two times a year, as well as once all together, at Europol’s headquarters in The Hague to share strategic information related to cybercrime threats and trends in their respective business areas, as well as to agree on joint initiatives alongside law enforcement. A current list of members can be found [here](https://www.europol.europa.eu/european-cybercrime-centre-ec3/ec3-partners).

[Download the report here](https://www.europol.europa.eu/sites/default/files/documents/report_on_phishing_-_a_law_enforcement_perspective.pdf)