Reporting phishing to authorities

Reporting phishing attacks to authorities is a crucial step in combating cybercrime. In this article, we'll explore why reporting phishing attacks is essential, and we'll provide insights into the challenges authorities face in catching these cyber pirates.

Why report phishing attacks to authorities?

- Protect yourself and others.
  The primary reason to report phishing attacks is to protect yourself and others from falling victim to the same scheme. Phishing attacks can lead to financial loss for the victims. When you report a phishing attempt, it allows cybersecurity experts to analyze the attack, identify its characteristics, create countermeasures and awareness to prevent others from being fooled by similar tactics, and sometimes to seize illegal gains, helping the recovery of stolen assets.

- Help legal action.
  Reporting phishing attacks helps justice gather evidence and build a case against cybercriminals. This can lead to criminal charges, arrests, and convictions, holding the perpetrators accountable for their actions. Such legal consequences serve as a deterrent to potential cybercriminals.

Fair warning: don't overestimate the action of the authorities in front of phishing. Unless you have suffered a real substantial financial loss, their action is rather limited. While reporting phishing attacks is essential, it's important to recognize that catching the perpetrators can be challenging due to several reasons:

- Anonymity: phishers often hide behind layers of anonymity, making it difficult to trace their real identities.

- Jurisdictional issues: phishing attacks can originate from different countries, creating jurisdictional challenges for police and justice. International cooperation still involves a ton of papework while sending an email across the globe is only a few milliseconds away.

- Evolving tactics: phishers constantly evolve their tactics to stay ahead of authorities, making it a constant game of cat and mouse.
- Limited resources: law enforcement and judicial organizations have limited resources to investigate every reported phishing incident, prioritizing more significant cases.

How to report phishing attacks to authorities?

- Report to cybersecurity agencies.
  Many countries have dedicated agencies or units responsible for handling cybercrimes. The following table lists some of them. If you do not see relevant information for you, please research the relevant agencies in your country and follow their reporting procedures.

Country	Information	Procedure
Belgium	https://www.safeonweb.be/en/useful-links	Forward or send as attachment the phishing email to suspicious@safeonweb.be For phishing via SMS (smishing), take a screenshot and send it to suspicious@safeonweb.be
France	https://www.signal-spam.fr/en/	Go to https://signalants.signal-spam.fr/login, create an account and follow the procedure
Germany	https://www.internet-beschwerdestelle.de/en/complaint/submit/e-mail-and-spam.html	Forward mail to besonderer-spam@internet-beschwerdestelle.de
EU	https://www.europol.europa.eu/report-a-crime/report-cybercrime-online	Enter the link of the fraudulent website on https://phishing-initiative.eu/contrib/
UK	https://www.gov.uk/report-suspicious-emails-websites-phishing	Forward mail to report@phishing.gov.uk Forward SMS to 7726
Switzerland	https://www.post.ch/en/about-us/responsibility/information-security-at-swiss-post/phishing-and-other-attempts-at-fraud-on-the-internet	Forward mail to reports@antiphishing.ch
USA	https://www.ftc.gov/business-guidance/small-	Forward mail to reportphishing@apwg.org

Country	Information	Procedure
	businesses/cybersecurity/phishing	Report fraud tentative on https://reportfraud.ftc.gov/#/assistant

- Report to the police (or equivalent law enforcement).
  If you have fallen victim of phishing and you suffered loss of money or identity, file a complaint with the police or equivalent law enforcement agency.

- Inform Your Bank and Credit Card Companies.
  If the phishing attack involved financial fraud, contact your bank and credit card companies immediately. They can freeze your accounts and initiate their own investigations, which can complement law enforcement efforts.

Conclusion

Reporting phishing attacks to authorities is a crucial step in the fight against cybercrime. While it may be challenging to catch phishing pirates due to the complexities involved, your report can contribute to the overall effort of strengthening cybersecurity and protecting individuals and organizations from falling victim to these malicious schemes. By working together and reporting incidents promptly, we can help make the internet a safer place for everyone.