GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

# Impact of COVID-19 on Financial Crimes

## Webinar 13.05.2020 - Q&A

**Q:** In addition to the DNS associated with a domain, the IPS and the use of Whois, Other additional methods are being studied actually, such as adding a digital identification certificate for each domain, for example, or other elements?

**INTERPOL**: To some extent I agree that domain certificates can help mitigate threats from domain imposters. The actual security benefit may vary depending on the details of implementation of the technology, such as who verifies what and how. A verified domain with HTTPS does not necessarily mean the physical entity has been validated. As discussed during the webinar, look-alike domain names such as interp0l.int (with number zero instead of letter o) may as well be validated. This is less than expected security that some users may expect from domain certificates. Having more security options are desirable, and more vigorous validation would be a lot more helpful. Still, we recommend that we should avoid depending on the domain certificates as actual security may be underprovided.

**Q:** Apart from Pol-Pol cooperation (through NCB or not) there could also be FIU-FIU cooperation especially re transactions related to fraud. What is your experience? Can you compare the two?

**INTERPOL** encourages all LEAs to use both channels concurrently as they are useful in following the money trail. However, as certain jurisdictions have strict banking secrecy laws that prohibits the sharing of banking information via the Pol-Pol channel, the FIU channel may come in handy to provide the said banking information for the purpose of conducting funds tracing and/or building up the financial profile of a suspect. Hence, we always encourage our National Central Bureaus (i.e. our points-of-contact for each country) to work closely with their respective FIUs to see if there any useful information that can be provided across either channel.

**Q:** For international fraud cases, it was highlighted by Jung Kee that acting quickly is important. what is the optimal timeframe as regards victim reporting and involvement of Law Enforcement to be able to trace the movement of money and freeze the bank account?

[the response to next question applies here as well]

**Q:** We know that electronic payments could be done on minutes in the case than a person could be victim on an international payment fraud. What should be the steps to response for that kind of incident? Is there are restrictions or specific conditions to investigate or response to that kind of incident?

**INTERPOL:** To address both questions, the general guideline would be for the victim to lodge a police report and submit a request to the bank to recall the funds within 48 hours. Beyond this, the likelihood of recovery may be low. Nonetheless, the requisite reports should still be lodged for other follow-up actions, including funds tracing and investigation of the beneficiary/recipient of the funds.

**Q:** I was wondering if you are aware of a criminal scheme that we have seen many times in Macedonia -where business e-mails are intercepted somewhere between the sender and receiver with the aim of changing the bank details for the transfer of money payable from the receiver to sender of email?

**INTERPOL:** Yes, we term this as Business Email Compromise Fraud, otherwise known as 'Invoice fraud'. You may wish to read further on it here: https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud. Further, perpetrators of this fraud have been seen to exploit the COVID-19 crisis.

**Q:** Just to make sure, any LEA in different countries has the ability to freeze a bank account without a judicial order?

**INTERPOL:** This is highly dependent on the countries' respective legislations, but most countries are able to freeze bank accounts without the need for a judicial order since this forms part of provisional measures, and not an action taken as part of an investigation. However, judicial orders may be required subsequently when it comes to formal seizure of the funds, or return of funds to the victim.

**Q:** How the threat actors are creating enormous numbers of COVID-19 domains anonymously and where they are hosted?

**INTERPOL:** Thousands of domain registrars will be happy to provide domain names at very low fees. You may see how ICANN is accommodating the domain industry here: https://www.icann.org/resources/pages/register-domain-name-2017-06-20-en

**COE:** The Registrars' Stakeholders Group of ICANN issued recommendations on how to identify potentially malicious domains related to COVID-19 and assess their possible harm: https://rrsg.org/wp-content/uploads/2020/03/Registrar-approaches-to-the-COVID-19-Crisis.pdf.
Statistics on the number of domains that are registered can be found through the COVID-19 Cyber Threat Coalition and their Weekly Threat Advisories: https://www.cyberthreatcoalition.org/.

**Q:** Dear Sir, good morning. Question for my Master's Thesis. Is there a possibility that terrorist organizations have used the health emergency COVID19 to find and / or recycle financial resources through virtual currencies? Thank you. Best regards. Claudio.

**INTERPOL:** It may or may not be possible, but we have no evidence to support this claim.

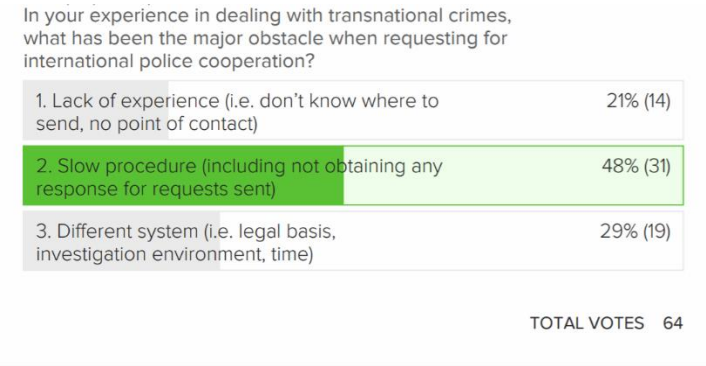
**Q:** Machine learning and deep learning algorithms are currently used to act against COVID19 that create opaque (black) boxes on Artificial Intelligence. What is your experience in the field of artificial intelligence and responsibility?

**INTERPOL:** As far as I know, statistical forecasting and its variants are in infancy in criminal justice field. Many challenges are there, beginning from lack of criminal statistics of law enforcement agencies, resulting too small data samples to start from. In wider information security area, ML has much more possibilities and we do see commercial products already, e.g. helping intrusion detection.

**COE:** That of Artificial Intelligence to support LE operations in the field of cybercrime is an interesting topic and we will dedicate to it one of our next webinars. Please follow our updates on our dedicated webpage (https://www.coe.int/en/web/cybercrime/webinars) and subscribe to receive our newsletters (https://www.coe.int/en/web/cybercrime/cyber-digests-and-updates)

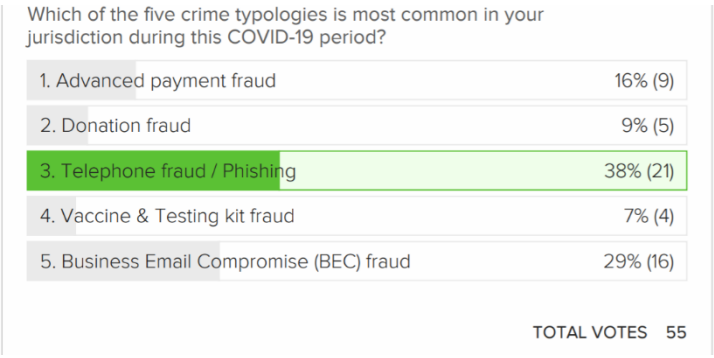
## POLLS

**First Question:**




This has been the most common issue that results may vary across jurisdictions, but we urge all countries to align its interest with the requesting country to ensure the same level of attention is given to international requests.

**Second Question:**




Telephone fraud / phishing was the first few crimes to have occurred during this crisis, and it still seems to be a common problem across the board. We urge all stakeholders to heed the advice provided.

## PANEL

**Dong Uk KIM**, Specialised Officer, GLACY+ project, Cybercrime Directorate, INTERPOL

**Muhammad IMRAN**, Criminal Intelligence Office, INTERPOL Financial Crimes Unit, INTERPOL Global Complex for Innovation (IGCI)

**Jung Kee YOU**, Criminal Intelligence Office, INTERPOL Financial Crimes Unit, INTERPOL Global Complex for Innovation (IGCI)

**www.coe.int/cybercrime**

INTERPOL
Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe