Iran: Identity Theft and Extortion in Isfahan

OE Watch Commentary: Traditionally, Iran's cybersecurity forces battle moral crimes such as pornography or those using social media for illicit political speech or activity. Increasingly, however, they appear focused on the rise of financial cybercrime inside Iran (see "Iran: Cyber Crime Rises," *OE Watch*, February 2016). In May 2018, for example, the Intelligence Ministry announced the arrest of hackers seeking to steal money from an Isfahan bank (see "Group Planning to Hack Bank in Iran Arrested," *OE Watch*, July 2018). This July, Iranian police warned of various telephone scams (see "Iran Warns of Phone and Text Scams," *OE Watch*, September 2019). In the excerpted article from Iran's cyber police homepage, the Isfahan cyber police branch announces that a complainant came to them to register charges of identity theft in an apparent phishing scheme that resulted in theft of their identity documents. The cybercriminal had then proceeded to harass and try to extort the complainant. The report also notes that the suspect was identified and summoned to the police.

To most non-Iranians, cyberthreats in Iran suggest Iranian attempts to hack critical infrastructure overseas or to steal personal information or to create fake social media profiles so as to gather intelligence on officials in Iraq and other countries. However, announcement of this case and the arrests suggests that Iranians increasingly suffer from domestic criminal hackers and that they appear to have confidence in the police to investigate certain cybercrimes. It is unclear whether pro-government hackers 'moonlight' in crimes against Iranians. So long as ordinary Iranians remain relatively naïve about cybersecurity, such as scanning the Iranian equivalent of social security cards or drivers' licenses onto their computers or phone, such crimes will continue. Indeed, as Iran's fiscal situation worsens, it is possible Iran will see a spike in cybercrime as financial desperation leads to more scams and online theft. **End OE Watch Commentary (Rubin)**

"Under no circumstance should anyone store his identity documents on smart devices."

Source: "Akhazi Internet ba Sareghat-e Ettela'at-e Havyati (Internet Extortion with Theft of Personal Identity Information)," *Mehr News Agency*, 23 November 2019. https://www.cyberpolice.ir/news/145615/اخاذی-اینترنتی-با-سرقت-اطلاعات-هویتی#no-back

Internet Extortion with Theft of Personal Identity Information

Cyberpolice Information Base: Colonel Mohammed Reza Hassanzadeh, head of the detection and prevention department, said in a statement, "After an individual complained that an anonymous person had a photo of his identity and identity information and sent threatening messages to extort him, and it came to police attention.

The official continued: Initial investigation revealed that an anonymous person had access to the plaintiff's profile image and identity information accessed with the plaintiff's access code, and by sending threatening messages, sought to extort the victim.

He mentioned: Based on victim statement and police action, the suspect was identified and summoned to the police with technical evidence. During the interrogation, the defendant said that "I was able to obtain a picture of his identity document by sending fake promotional messages and gaining the credentials of the plaintiff by accessing the profile." Colonel Hassanzadeh said, "Under no circumstance should anyone store his identity documents on smart devices at all."

Sepah Bank in Isfahan.
Source: Contemporary Architecture of Iran, http://caoi.ir/images/igallery/resized/3501-3600/Sepah_Bank_in_Isfahan_Iran_by_Vartan_Hovanesian__1_-3549-800-500-100.jpg