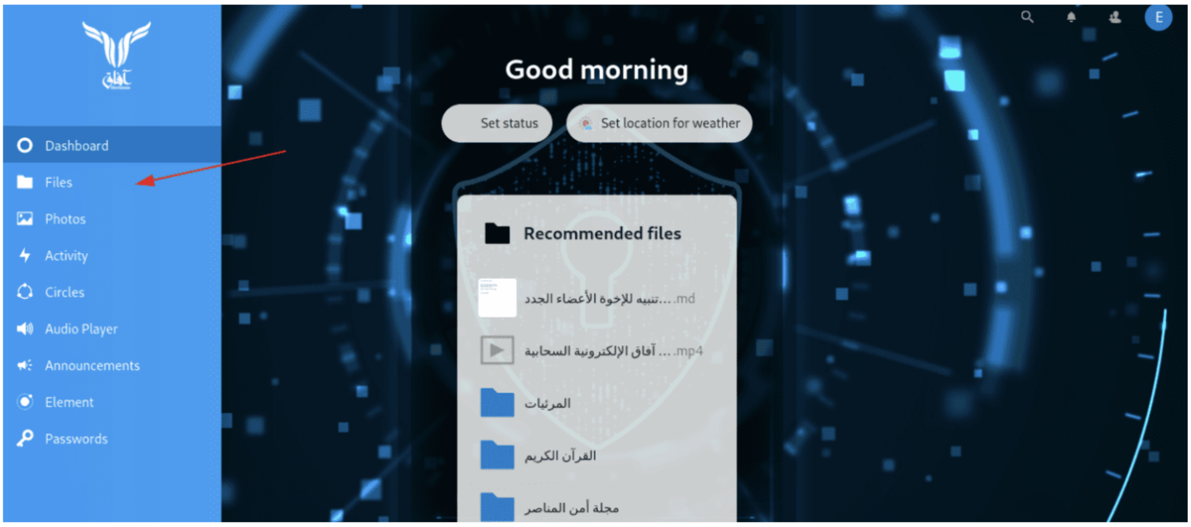
GTSC Government Technology & Services Coalition's HOMELAND SECURITY TODAY.US

ISIS Cyber Group Launches Cloud, Chat Platforms to 'Close Ranks' Online

April 6, 2021 Bridget Johnson



An ISIS-supporting cybersecurity group launched their own cloud and chat platforms that they vowed would help churn out new propaganda and allow followers of the terror group to better "close ranks" online.

"In light of recent developments in the media arena and the restriction of technology companies to content, we resorted to developing solutions that provide a space for propagation between the fellow supporters and the general Muslim community, so that the benefits may prevail," the Electronic Horizons Foundation said in its announcement posted online. "We developed the 'Horizons Cloud Platform' for advocates to use to upload and publish files on the Internet."

The group also developed an Element-based messaging and chat hub "to provide publishing rooms and continuous follow-up for news and content as an initiative to close ranks, and a starting point for the development of media work, Insha Allah."

"Note that our technical support teams are fully prepared to guide the brothers to solve technical and security problems, Insha Allah," the group added. "We pray to Allah to guide us to what is right and to help us against our enemies."

The announcement, which was published in English, Arabic, French, and Italian, includes links to the platforms and ISIS tech support contacts on Element, XMPP, Threema, and Telegram in case supporters have problems registering.

The Electronic Horizons Foundation launched in January 2016 as an IT help desk of sorts to walk ISIS supporters through how to encrypt their communications and otherwise avoid detection online while coordinating with and recruiting jihadists.

EHF released a 24-page cybersecurity magazine for ISIS supporters last May that walks jihadists through step-by-step security for smartphones — while encouraging them to use a computer instead for more secure terror-related business — and warns of “nightmare” Microsoft Windows collecting user data from geolocation to browsing history.

The group regularly issues cyber news, guidelines and advisories, such as an “important warning” earlier this year telling supporters that “spies of intelligence agencies are using a new method to track down supporters through Google Play Store.”

In an online tutorial intended to walk users through the registration process for the new cloud platform, which uses German company Nextcloud’s software, the group includes a “caution” that the platform “is for uploading media files, and it’s not for uploading personal files.”

“We have no responsibility for using them in what isn’t pleasing to Allah,” the group adds.

For registration, the group advised ISIS supporters to “use a new e-mail from Protonmail.com or Tutanota.com services or other encrypted mail services to create an e-mail for uploading only on the site with the use of VPN services or the Tor network.”

New registered users were advised to go into settings and make their account data private. The tutorial walks users through how to create files, add icons, generate a public link for the file, and then share that on social media sites. “We recommend that users of smartphones (Android – iPhone) use the platform through the browser,” the group noted.

Files on the tutorial screen included The Supporter’s Security, the cyber magazine previously released by EHF, and a library of other releases from the cyber group. There is also a section for announcements where the group said it would post new updates on the cloud platform.

The chat interface home screen promises to “liberate your communication” and gives options for sending direct messages, exploring public rooms, or starting a group chat.

EHF last year urged followers to use alternate operating systems such as Qubes, Tails or Whonix. The ISIS cyber group has also highlighted “wrong security practices” including browsing the internet without Tor or VPN, downloading apps from third-party sources, failing to encrypt the device or storage devices, neglecting to install security updates, failing to use fake credentials on social media, and using social media via apps instead of logging on through a browser. Jihadists have also been warned against opening potentially malicious links that can open them to a security breach.

The EHF has released a series of print and video tutorials covering a range of mobile security and dark-web how-tos for fellow ISIS supporters, along with weekly tech bulletins to educate ISIS followers about current cybersecurity trends and vulnerabilities.