GDPR & Security

Mandating more cookie pop-up notices does not mean that your data is more secure.

The GDPR enables bad actors to hide in the shadows. To comply with the new regulation, ICANN announced that it will allow registries and registrars to obscure WHOIS information, making it harder to identify the culprits behind harmful domains.

- The WHOIS database holds information on who runs domains, making it a useful tool for law enforcement to track crime. Since its system has become more anonymized through a Temporary Specification following the GDPR, security professionals worry that it'll be harder to hold criminals accountable.
- Since the ICANN's Temporary Specification was enacted, billions of users have been exposed to online scams for significantly longer periods than in a pre-GDPR world.
- One security company found that following the change to the WHOIS system, its success rate for obtaining registrant information is only 49%.
- As of July 2019, the company found "full, un-redacted" registrant information for only 6% of violating domains.
- IBM X-Force reported a 91% decrease in researchers being able to successfully block bad actors. In October 2017, researchers were able to block about 1.8 million newly registered harmful domains. By February 2019, that number dropped to less than 160,000.

Under the GDPR, users can request all of their data from a company. However, the law's lack of user authentication provisions and tight deadlines and regulations on organizations leave this process vulnerable to hackers, identity thieves, and even just human error.

- After hackers break into a user's account, they can now easily access all of that user's personal information. Jean Yang, a computer science professor at Carnegie Mellon University, discovered that hackers were able to request and download her music streaming history, date of birth and payment information after breaking into her Spotify account.
- Oxford University student James Pavur demonstrated how easy it is to steal user data through the GDPR. He sent a simple email that included the name, email and phone number of his fiancée and paper co-author to 150 organizations.
    - 24% of the organizations gave him the information right away.
    - 16% provided the information after requesting weak forms of authentication, which he was able to complete.
    - 3% automatically deleted his fiancée's account to avoid dealing with the data request.
    - Just through sending a basic email, he was able to collect her personal information — including her stays at a popular hotel chain and even her social security number.

- After one German man requested his data from Amazon, he received over 1,700 Alexa voice recordings of another user. The original requester turned the files over to a German magazine after he was unable to get in touch with Amazon. There, reporters were able to piece together who the identities of the other recorded man and his female companion. Though Amazon claims this was human error, it demonstrates how GDPR's provisions enable potentially sensitive information to get in the wrong hands.

For more information on why GDPR-style regulation would be bad for American businesses and consumers, contact Katie McAuliffe at kmcauliffe@atr.org.