March 23, 2020

DoJ to Aggressively Address Fraud, Cyber Scams Related to Pandemic

The Department of Justice has promised to aggressively pursue fraud and cyber scams that seek to capitalize on public concern about the ongoing coronavirus pandemic, and over the weekend DoJ won a court's permission to shutter a website that had been selling a bogus coronavirus vaccine.

"Attorney General [William] Barr has directed the department to prioritize fraud schemes arising out of the coronavirus emergency," said John F. Bash, U.S. attorney for the Western District of Texas. "We therefore moved very quickly to shut down this scam. We hope in the future that responsible web domain registrars will quickly and effectively shut down websites designed to facilitate these scams."

U.S. District Judge Robert Pitman issued a temporary restraining order requiring that the registrar of the website, "coronavirusmedicalkit.com," immediately take action to block public access to it. Operators of the website claimed to offer access to World Health Organization (WHO) vaccine kits in exchange for a shipping charge of $4.95, which consumers would pay by entering their credit card information on the website, DoJ said. There is no vaccine yet for the virus causing the global pandemic, known as COVID-19.

"The Department of Justice will not tolerate criminal exploitation of this national emergency for personal gain," said Jody Hunt, the assistant attorney general in charge of DoJ's Civil Division. "We will use every resource at the government's disposal to act quickly to shut down these most despicable of scammers, whether they are defrauding consumers, committing identity theft, or delivering malware."

A criminal investigation into the website is ongoing; DoJ's Civil Division shut the site down using a federal statute that allows federal courts to issue injunctions to prevent harm to potential victims of fraudulent schemes.

DoJ and other entities are reiterating advice that many Internet users have heard before – that they should keep their systems patched and up-to-date, should be careful about clicking on unknown links, look out for websites that try to mimic legitimate government websites (such as "cdc.com" versus "cdc.gov"), and be skeptical about coronavirus-related sales pitches.

USTelecom, for example, today offered an infographic on cybersecurity for the public and for its member companies to offer to their customers, many of whom are now working remotely on systems that might be less secure than those in the workplace. The "6 Tips to Thwart COVID-19 Cyberscams" infographic advises Internet users to "Think Before You Click" and "Turn on Auto Updates." —Tom Leithauser, tom.leithauser@wolterskluwer.com