## Fake online pharmacies “catch” patients through the sheer volume of websites they run.

95% of online pharmacies are unsafe,[1] which is why patients who search for medicine online often end up on fake online pharmacy websites. As early as 2011, **30 criminal networks were running 54,220 websites** named things like “Pharmacy Express” to trick users into buying fake medicines and/or catch them in phishing, spam, and malware schemes.[2]

**Domain name registry companies** (which handle domain extensions like .com, .edu, and .org) and **domain name registrars** (which sell domain names to the public) control the web addresses these networks depend on.

## Covid-19 has triggered an avalanche of new domains named to cheat people seeking help in the pandemic.

In the first quarter of 2020, **domain name sellers took money for more than 115,000 COVID-19-related domain names**, many of which are for sites selling black market face masks and hand sanitizer, fake COVID-19 tests or vaccines, and other unregulated pharmaceuticals.[3] New COVID-19- themed domain names are being registered at 1,000 per day.[4]

Sites like these part many vulnerable people from their money but **they can also kill COVID patients** by selling fake products which neither protect them nor treat COVID-19.

## Companies that host or sell domain names have the power to stop COVID scammers, but they haven’t stepped up.

### ACT NOW

Tell Congress to give Law Enforcement the power to identify scam domain owners and get them off the Internet.

TEXT STOPSCAM to 52886 to send a letter to your members of Congress or go to www.safemedicines.org and write a letter there.

### ACT NOW

Historically, many of these companies have put profit over safety even when a domain name implies illegal activity, violates their terms of use, or sells opioids or COVID-19 “cures.”[5] This puts lives at risk, especially in a public health emergency when millions are relying on the internet for healthcare information, products, and services.

These companies also maintain a database called WHOIS, which keeps contact information for who has registered domain names. Until 2018, investigators used WHOIS to track down cybercriminals, but in the last two years access to WHOIS has been radically limited in response to EU privacy laws and other policy changes. As a result, authorities cannot find and prosecute those selling fraudulent products on websites like “corona-cure.com,” “northern-pharmacy. com,” or “buytramadolpills.com.”[6] Counterfeiters hurting patients might lose a website, but they can just register a new one. Or another 10,000.

## Frequently Asked Questions

**The world wide web is worldwide. Won't regulating activity in the U.S. just drive crime off-shore?**
Most domain names touch a US-based company at some point along the way, so a law in the U.S. would have an immediate beneficial impact on public safety. Additionally, it would serve as a model law to take overseas to other countries where criminals might look to register domain names.

**Why shouldn't people need a court order to get WHOIS information?**
WHOIS was an open record of who owned Internet real estate for over thirty years, much like public land titles in the 'real world.' Ordinary citizens and watchdog nonprofits use this information to protect themselves and the public but wouldn't have access under a model where only a court order can be used to get information.

Legitimate public access protects consumers. The WHOIS database is crucial for identifying, prioritizing and allocating resources for policing malicious and unlawful activity on the Internet. Limiting access will lead to a significant rise in cyberattacks and fraudulent online activity that law enforcement, cyber researchers, companies or consumers cannot respond to.

**Privacy is important, but so is stopping illegal activity on the Internet.**

[1] National Association of Boards of Pharmacy, "Internet Drug Outlet Identification Program Progress Report for State and Federal Regulators: September 2018."

[2] K. Levchenko *et al.*, "Click Trajectories: End-to-End Analysis of the Spam Value Chain," *2011 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2011.

[3] "Don't Panic: COVID-19 Cyber Threats." Palo Alto Networks Unit 42 blog, March 24, 2020. "ICE HSI launches Operation Stolen Promise," U.S. Immigrations and Customs Enforcement, April 15, 2020.

[4] "Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN." *Interisle Consulting Group, LLC*, March 31, 2020, page 18.

[5] FDA Presentation at ASOP Global Foundation Research Symposium, November 2018; See also FDA Registry and Registrar Abuse Complaints.

[6] Letter from the Center for Drug Evaluation and Research and the Federal Trade Commission to Corona-cure.com, March 27, 2020.