Microsoft

Digital Crimes Unit

Leading the fight against cybercrime

750% - growth in ransomware families in 2016

$3.6 Million – average cost of data breach in 2017

$8 Trillion - estimated cost of cybercrime to the global economy by 2022

Innovating with technology and law

Microsoft's Digital Crimes Unit (DCU) is an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals focused on protecting people, organizations and our cloud against cybercriminals. We disrupt cybercrime through the innovative application of technology, forensics, law and partnerships.

DCU Areas of Focus

Tech Support Fraud – We use a data-driven approach to understand and investigate tech support fraud criminal networks, take legal action and refer cases to law enforcement. We apply what is learned to further secure our customers through technology and educate consumers on how to stay safe online.

Online Child Exploitation – We equip law enforcement, tech companies and others with PhotoDNA to help detect and disrupt the distribution of child sexual abuse materials. PhotoDNA technology results in more than 9 million CyberTips to the National Center for Missing & Exploited Children (NCMEC) annually.

Cloud Crime and Malware – We identify, investigate and disrupt malware and other criminal activity impacting devices globally. We embed the intelligence from our operations into our products and services to make them more secure, and work with Computer Emergency Response teams to notify and clean victim devices.

Global Strategic Enforcement – We target global cybercriminal networks involved in the theft of customer credentials, unlawful use of cloud services, and misappropriation of Microsoft intellectual property. Our objective is to disrupt and dismantle these criminal networks thru referrals to law enforcement and civil actions.

Nation-State Actors – We use creative technical and legal strategies to disrupt the criminal infrastructure, deter nation-state actors from using our platform, and notify victims of these cyber-attacks.

Public/Private Partnerships

Fighting cybercrime across borders

Cybercrime is border-agnostic and impacts victims globally. Law enforcement's authority is constrained by jurisdiction and antiquated processes used to request cross-border collaboration and information. Fighting cybercrime requires strong international public/private partnerships and orchestration.

DCU's Cybercrime Center serves as a global hub where Microsoft can come together with law enforcement, NGOs, industry, academics and security firms, to fight cybercrime. Joining together in operations across our programs, we can follow leads, look for attribution, identify victims, and disrupt the criminal's infrastructure. We are able to act faster to stop harm to customers, and develop evidence that law enforcement can use to focus on arrests and convictions.

> *"The clear message is that public-private partnerships can impact these criminals and make the internet safer for all of us."*
>
> –Steven Wilson, Head of Europol's Cybercrime Center

Resources

The Microsoft News Center:
https://news.microsoft.com/presskits/dcu

Microsoft Secure:
https://www.microsoft.com/security

Microsoft Safety & Security Center:
https://www.microsoft.com/safety

Data Sources:
A Record Year for Enterprise Threats (TrendMicro February 2017 Report)
2017 Cost of Data Breach Study: Global Overview
The Future of Cybercrime & Security: 2017-2022 (Juniper Research)

The DCU is committed to protecting the privacy of individual and enterprise data while aggressively fighting cybercrime targeting our customers, our cloud, and our company.