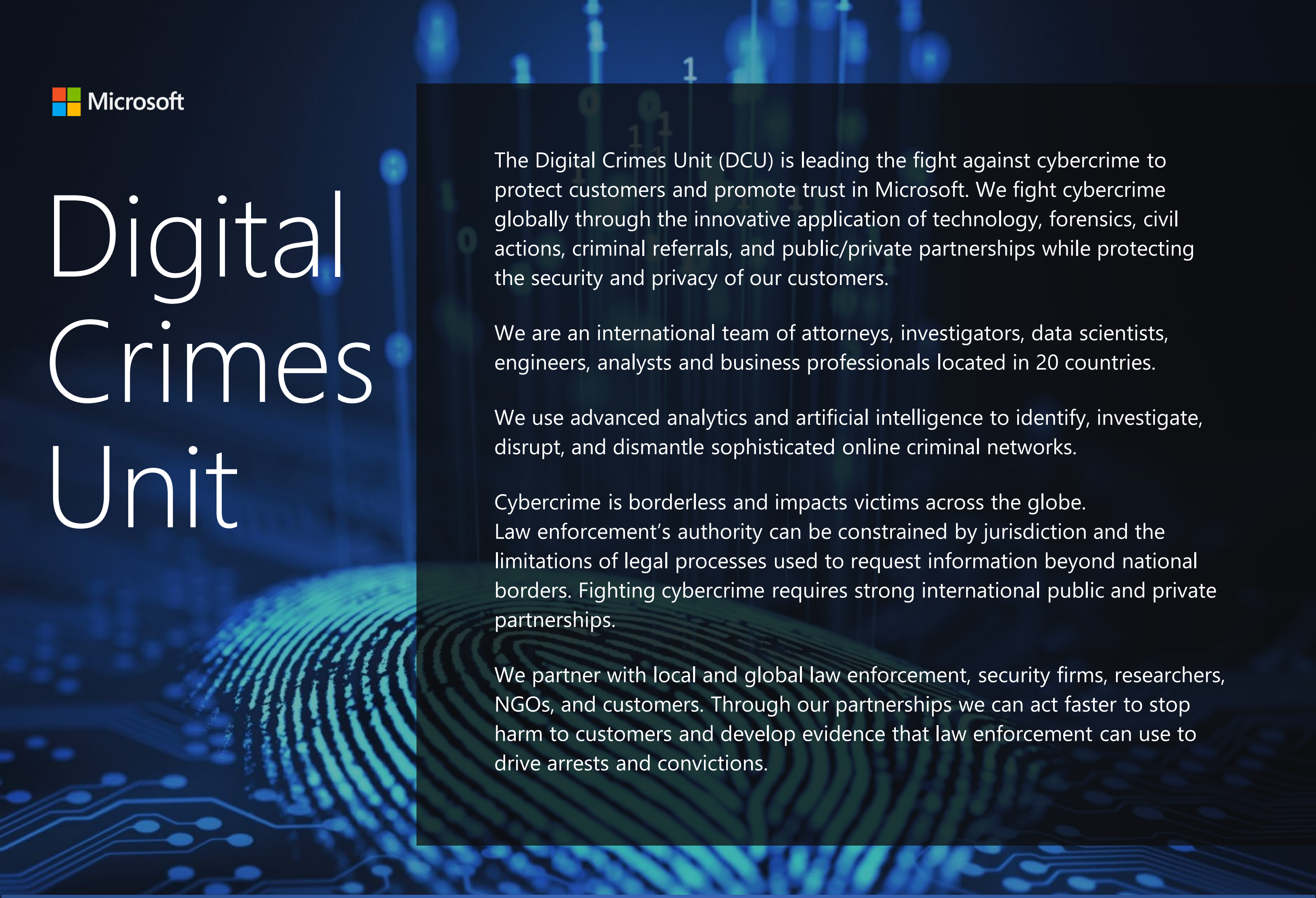

Digital Crimes Unit

The Digital Crimes Unit (DCU) is leading the fight against cybercrime to protect customers and promote trust in Microsoft. We fight cybercrime globally through the innovative application of technology, forensics, civil actions, criminal referrals, and public/private partnerships while protecting the security and privacy of our customers.

We are an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals located in 20 countries.

We use advanced analytics and artificial intelligence to identify, investigate, disrupt, and dismantle sophisticated online criminal networks.

Cybercrime is borderless and impacts victims across the globe.
Law enforcement's authority can be constrained by jurisdiction and the limitations of legal processes used to request information beyond national borders. Fighting cybercrime requires strong international public and private partnerships.

We partner with local and global law enforcement, security firms, researchers, NGOs, and customers. Through our partnerships we can act faster to stop harm to customers and develop evidence that law enforcement can use to drive arrests and convictions.

The Digital Crimes Unit focuses on the following areas:

Cloud Crime and Malware

In partnership with threat intelligence and security experts across Microsoft, the DCU applies unique legal and technical solutions to identify, investigate, and disrupt malware-facilitated cybercrime and nation-state sponsored activity.

- Since 2010, the DCU has collaborated with law enforcement and other partners on 22 malware disruptions, resulting in over 500 million devices rescued from cybercriminals.
- The DCU's malware disruption operations are powered by Azure, providing unrivaled computing power.
- Traffic from victim devices that once communicated to criminal servers is safely rerouted to Microsoft's Cyber Threat Intelligence Program (CTIP). Victim devices are cleaned through antivirus programs such as Windows Defender Antivirus or intelligence is shared with Computer Emergency Response Teams (CERTs) and Internet Service Providers (ISPs) around the world to notify victims and assist with removal of the malware.

NATION-STATE

- In 2016, the DCU used a civil action to disrupt a nation-state actor called Strontium, or Fancy Bear, that had leveraged Microsoft-like domains for spear phishing attacks, enabling the criminals to install a remote access kit that could be used to exfiltrate sensitive data.
- The DCU obtained a court order to re-direct the Microsoft-like domains leveraged by Strontium to a sink-hole. We were able to protect potential victims from losing their data to cybercriminals.
- We were also able to stop continuing spear-phishing attacks by Strontium by seeking appointment of a Special Master to expedite additional motions as new domains were registered by Strontium, with a response from the court in 24 hours or less.

Global Strategic Enforcement

The DCU's Global Strategic Enforcement Team (GSET) identifies, investigates, and takes enforcement against sophisticated global online criminal networks who specialize in business email compromise (BEC), stealing credentials, and online fraud.

- 90% of intrusions begin with an email. BEC is a growing threat to our customers and online commerce. The DCU is investing heavily in its enforcement program to identify, investigate, and disrupt BEC attacks while supporting the prosecution of responsible cybercriminals.
- Numerous schemes are designed to improperly access and misuse customer account credentials. Cybercriminals frequently seek to compromise accounts to fraudulently transact business or facilitate further cybercrime.
- GSET tackles online fraud to protect our customers and services. Cybercriminals frequently seek to fraudulently gain access to Microsoft programs that are intended to benefit students, underserved communities, and aspiring entrepreneurs. Online fraud schemes not only hurt Microsoft but also people and communities in most need of support.

Tech Support Fraud

The DCU leverages data analytics and machine learning to investigate criminal networks engaged in tech support fraud. We take legal action and refer cases to law enforcement and apply what is learned to strengthen our products and services and educate consumers on how to stay safe online.

- According to a 2018 Microsoft global online survey (https://aka.ms/TechSupportScamResearch), 3 out of 5 people globally have experienced a tech support scam.
- Scammers attempt to convince victims to provide remote access to their devices by impersonating a wide range of reputable technology companies, such as Apple, Google and Microsoft. Victims spend hundreds of dollars on these phony tech support services.
- Leveraging complaints received directly from consumers and pop-up advertisements scraped and classified through machine learning tools, Microsoft investigates criminal networks behind this global scam. We refer cases to law enforcement and take legal actions ourselves to protect our customers.
- Microsoft helps to educate consumers on how to stay safe online on the Windows Security Support site (https://www.microsoft.com/safety) and through partnerships with trusted organizations.

Online Child Exploitation

Microsoft equips technology companies and others with PhotoDNA to help detect, disrupt, and report the distribution of child sexual abuse images and videos.

- In 2009, Microsoft partnered with Dartmouth college to develop the hash matching technology known as PhotoDNA. This hashing and matching process makes it possible to effectively detect and disrupt illegal images of child sexual exploitation from the hundreds to billions of images that may be uploaded to an application or online platform daily. Over 150 organizations across the globe are using PhotoDNA today.
- PhotoDNA technology resulted in more than 10 million CyberTips to the National Center for Missing & Exploited Children (NCMEC) in 2017 alone.
- Microsoft continues to innovate to combat online child exploitation including developing PhotoDNA in the cloud and applying PhotoDNA to video.

For more on the DCU, visit:

Microsoft **On the Issues**
https://news.microsoft.com/on-the-issues/topic/cybersecurity/

https://twitter.com/MSFTIssues

DCU On **YouTube**
https://youtube.com/DCUMicrosoft

PhotoDNA
https://www.microsoft.com/photodna

Additional Resources:

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

Windows **Defender**
https://www.microsoft.com/wdsi

Windows **Security Support**
https://www.microsoft.com/safety