Microsoft

Digital Crimes Unit

Fact Sheet

Digital Crimes Unit Overview

Through enforcement actions, the Microsoft Digital Crimes Unit (DCU) works to safeguard people and organizations from digital threats.

- We are an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals working together to transform the fight against cybercrime.
- The DCU uses creative legal strategies and cutting-edge data analytics to build civil cases and criminal referrals, partnering with law enforcement worldwide, NGOs, industry, security vendors and researchers so that cybercriminals are brought to justice.
- In every phase of our operations, we are committed to the privacy of individual and enterprise data and helping protect our customers, our cloud, our company and the most vulnerable users of the internet.

Tech Support Fraud

Microsoft partners with law enforcement globally to investigate and take action against scammers, while working with advocacy groups to educate customers.

- According to a Microsoft global online survey, two-thirds of people have experienced tech support fraud.
- An estimated 3.3 million people in the United States are affected by this type of consumer fraud with losses of more than $1.5 billion annually.
- Scammers attempt to convince victims to spend hundreds of dollars on phony tech support services by impersonating companies such as Microsoft, Google and Facebook.
- Microsoft works closely with AARP's Fraud Watch Network, inviting AARP members to join monthly tours of Microsoft's Cybercrime Center, bringing expertise to AARP's Cyber Safety events, and publishing a brochure providing tips to seniors on how to safeguard themselves and take action if they have been a victim.
- Since 2014, Microsoft has received more than 180,000 reports of fraudulent tech support scams from customers around the world. Anyone who has been contacted by a potential scammer is encouraged to report their experience using this form. This information assists the DCU and law enforcement in their investigations targeted at stopping these scams.

Cloud and Datacenter Enforcement

Microsoft investigates and disrupts malware and other criminal activity that impact devices connecting to our cloud services, ensuring our datacenters are secure. We embed the intelligence we gather from our disruptions into our products and services to make them more secure.

- Every second, 12 people online become a victim of cybercrime, totaling more than 1 million victims around the globe every day.
- Malware costs the global economy $3 trillion in lost productivity and growth each year.
- It typically takes more than 140 days to detect infiltration.
- The average cost of a data breach is $4 million.
- Since 2010, Microsoft has worked with law enforcement and industry, leveraging novel legal strategies to disrupt the cybercriminals and help secure peoples' devices.
- As a result of the DCU team's malware disruption cases, tens of millions of infected devices connecting to more than 50 million internet protocol addresses have been rescued.
- Microsoft uses the computing power of Windows Azure and big data tools to fight cybercrime and shares this intelligence with law enforcement and those responsible for critical infrastructure in a country.
- Working with law enforcement and other partners, the DCU uses civil law to take action against the cybercriminals while law enforcement seizes the physical infrastructure.
- As a result of DCU's malware disruption cases, traffic that once communicated to criminal servers is safely rerouted to Microsoft's Cyber Threat Intelligence Program (CTIP) in our secured and trusted cloud.
- It is also shared with computer emergency response teams (CERTs) around the world that work with ISPs to notify victims and help clean infected devices.
- Data gleaned from this traffic is built into Azure Active Directory Premium, providing further protection for customers.

Online Child Exploitation

Microsoft enables law enforcement and organizations to detect and disrupt the distribution of child sexual abuse materials online by leveraging PhotoDNA, a scalable Microsoft technology.

- Approximately 720,000 abusive images are uploaded to the internet every day.
- PhotoDNA converts images into a greyscale format, then divides the image into squares and assigns a numerical value, or hash, that represents the unique shading found within each square. These hashes are then matched against a database of known illegal images.
- PhotoDNA technology can't be used to identify a person or object in an image. It is not facial recognition software. A PhotoDNA hash is not reversible and therefore cannot be used to re-create an image.
- PhotoDNA is available on-premises and in the cloud. It is provided free of charge to qualified companies, organizations and forensic tool developers.
- Currently, more than 100 companies including Facebook and Twitter, nongovernmental organizations, and law enforcement use PhotoDNA.

Global Strategic Enforcement

Microsoft uses sophisticated digital investigation and advanced analytics to develop civil actions and criminal referrals, protecting Microsoft services and customers against criminal organizations.

- Microsoft takes enforcement actions around the world to stop unscrupulous merchants and criminal syndicates from selling unlicensed and counterfeit software to unsuspecting customers
- People and/or enterprise organizations expose their networks and devices to digital risk when unlicensed software makes its way into their environment.
- Risks can include, but are not limited to, compromised IT security, increased exposure to malware and increased costs.
- Enterprises will spend more than a billion dollars in dealing with security issues as a result of malware associated with pirated software.
- Enterprises will spend billions of additional dollars dealing with data breaches that occur because of malware associated with pirated software.
- Microsoft can provide organizations with a view of the risk it sees in their environment by analyzing data sets unique to the DCU.

Additional Resources

- Newsroom
- Twitter
- YouTube
- Microsoft Safety & Security Center
- PhotoDNA
- AARP Fraud Watch Network