Microsoft

Digital Crimes Unit

Fact Sheet

Digital Crimes Unit Overview

Microsoft's mission is to empower every person and organization on the planet to achieve more. Every person and organization has the right to expect the technology they use is secure and delivered by a company they can trust.

- The Microsoft Digital Crimes Unit (DCU) helps meet this promise by fighting global malware, reducing digital risk and protecting vulnerable populations.
- The DCU combines big data analytics, cutting-edge forensics and novel legal strategies to protect your data, keep you in control of personal information, and help keep seniors and children safe online.
- The DCU is an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals based in 30 countries, all working together to transform the ongoing fight against digital crime.

Protection From Cybercriminals

Cybercriminals hijack devices, steal personal information, send spam, run phishing scams and target bank accounts. It's a global problem and no one organization can solve the issue of cybercrime on its own.

- 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.
- Since 2010, Microsoft has worked with law enforcement and industry, leveraging novel legal strategies to disrupt the cybercriminals and put people back in control of their 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.

Gathering and Sharing Intelligence via Microsoft's Cyber Threat Intelligence Program

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.

- Data gleaned from this traffic is built into Azure Active Directory Premium, providing further protection for customers.
- 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.

Fighting Tech Support Scams

Microsoft is fighting back through education, partnerships with government and law enforcement, and, when appropriate, direct legal action against scammers.

- 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 misrepresenting 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.

Protecting Children Online with PhotoDNA

Microsoft PhotoDNA technology, created in partnership with Dartmouth College, helps detect and disrupt the distribution of child sexual abuse materials online.

- 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.

Reducing Digital Risk

Microsoft is committed to sharing data insights, processes and recommendations that can reduce customers' exposure to digital risk.

- 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.
- As reported by the IDC, enterprises will spend $127 billion in dealing with security issues as a result of malware associated with pirated software.
- Enterprises will spend an additional $364 billion 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
- Facebook
- Twitter
- YouTube
- Microsoft Safety & Security Center
- PhotoDNA
- AARP Fraud Watch Network