CYBERSECURITY AND CYBERBULLYING

ERASMUS+

Ioannis Yerou
Information Security Manager

16/03/2021

University of Cyprus

Imperial College London

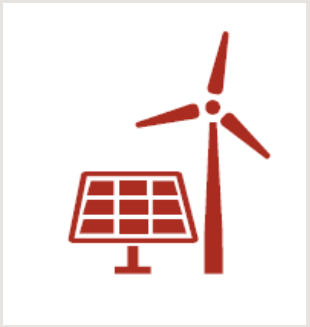
KIOS Research and Innovation Centre of Excellence

KIOS CENTER OF EXCELLENCE AT A GLANCE

- KIOS was established as a research unit in 2008 and upgraded to a Center of Excellence (CoE) in 2017
- Operates within the University of Cyprus (at the level of Faculty)
- Collaborates strategically with Imperial College, London
- Currently over 160 people at KIOS CoE
- Creates synergies with national and international industrial and governmental organizations

KIOS COE SCIENTIFIC AND INNOVATION POTENTIAL

- Technical focus & specialization
  - Intelligent monitoring
  - Control
  - management and security of complex, large-scale, dynamical systems
- Application Areas ➡ Critical Infrastructure Systems



Energy & Power Systems

Water Systems

Telecommunication Systems & Networks

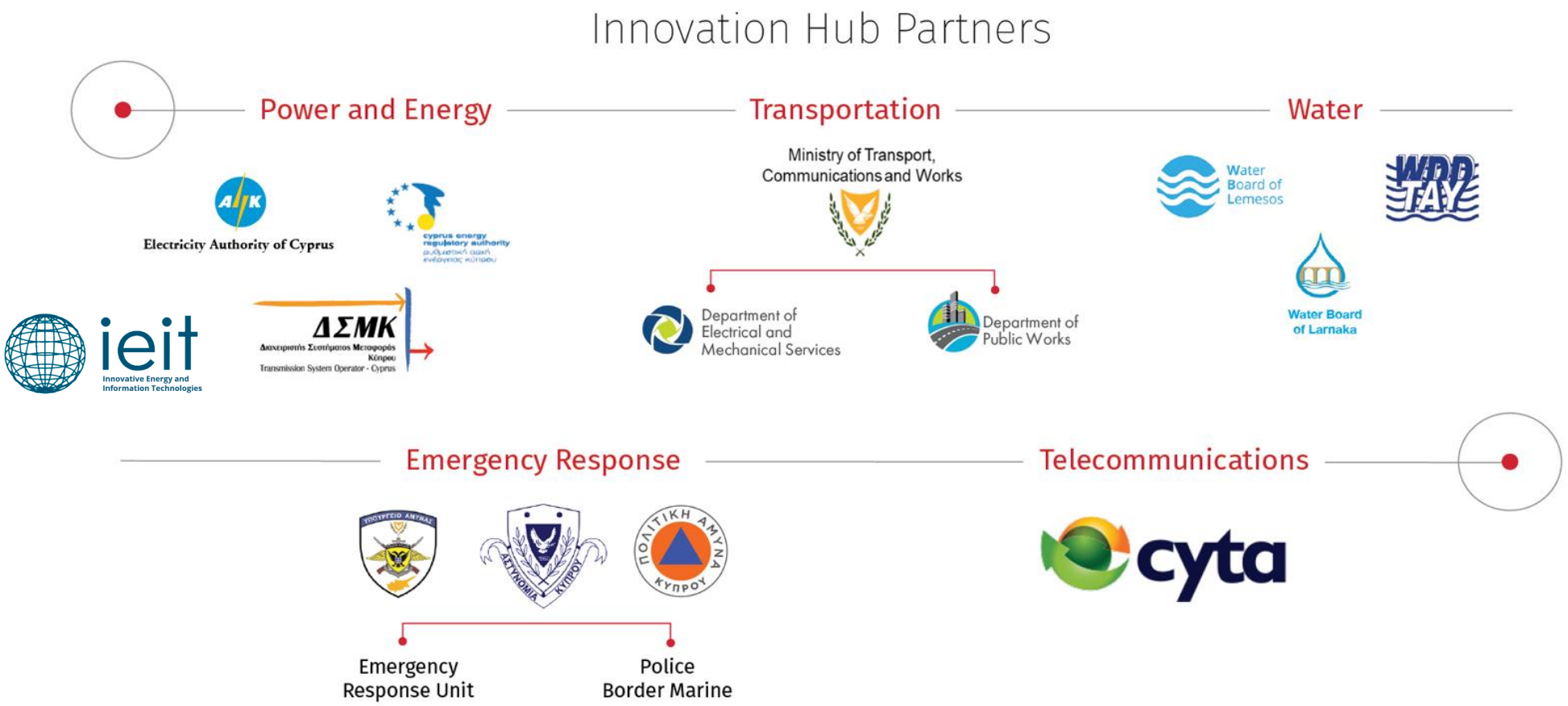
Intelligent Transportation Systems

Emergency Management Response

PROJECT ACTIVITY

- Over 30 active multi-disciplinary research projects funded by international, EU and national sources
- Projects are delivered in collaboration with industry and SMEs
- Contribute to global and regional challenges
- Smart Specialization Strategy


KIOS INNOVATION HUB – INDUSTRY PARTNERSHIPS



1. CYBERSECURITY

- Cybersecurity is the practice of protecting systems, networks, programs and associated data from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
- Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

WHAT IS CYBERSECURITY ALL ABOUT?

- A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe.
- In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.
- Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.
- Organizations must have a framework for how they deal with both attempted and successful cyber attacks. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

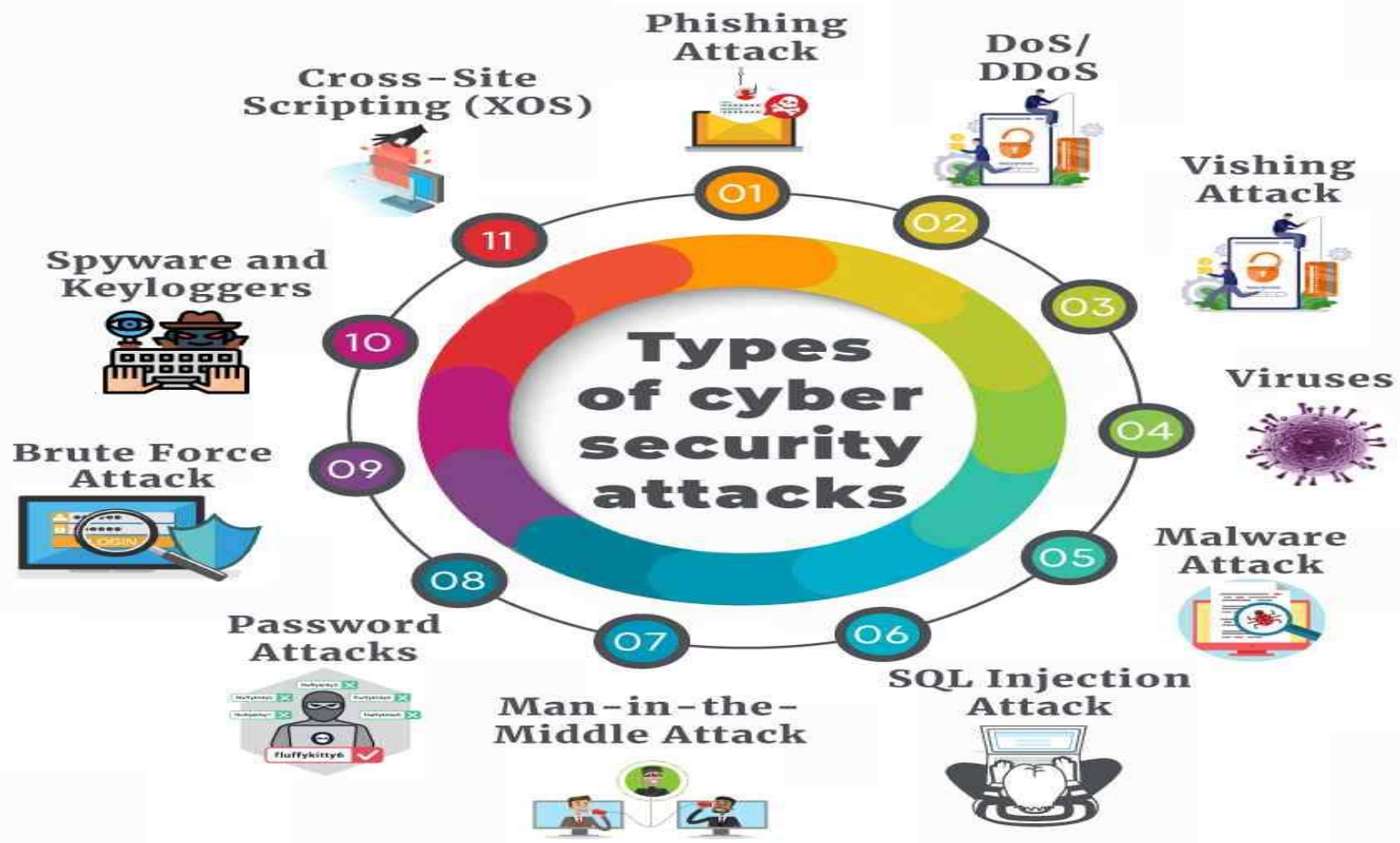
TECHNOLOGY AND HUMAN FACTOR

- Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Three main entities must be protected:
  - endpoint devices like computers, smart devices
  - Routers, networks
  - cloud
- Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.
- Technology alone is not enough. Educating the people using the technology and carrying out awareness programs are of crucial importance.

WHY IS CYBERSECURITY IMPORTANT?

- In today's connected world, everyone benefits from advanced cyber-defense programs. Anybody can initiate an attack from anywhere in the world.
- At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of confidential data.
- Everyone relies on critical infrastructure like power plants, hospitals, financial service companies, institutions. Securing these and other organizations is essential to keeping our society functioning.

TYPES OF CYBERSECURITY THREATS



TYPES OF CYBERSECURITY THREATS

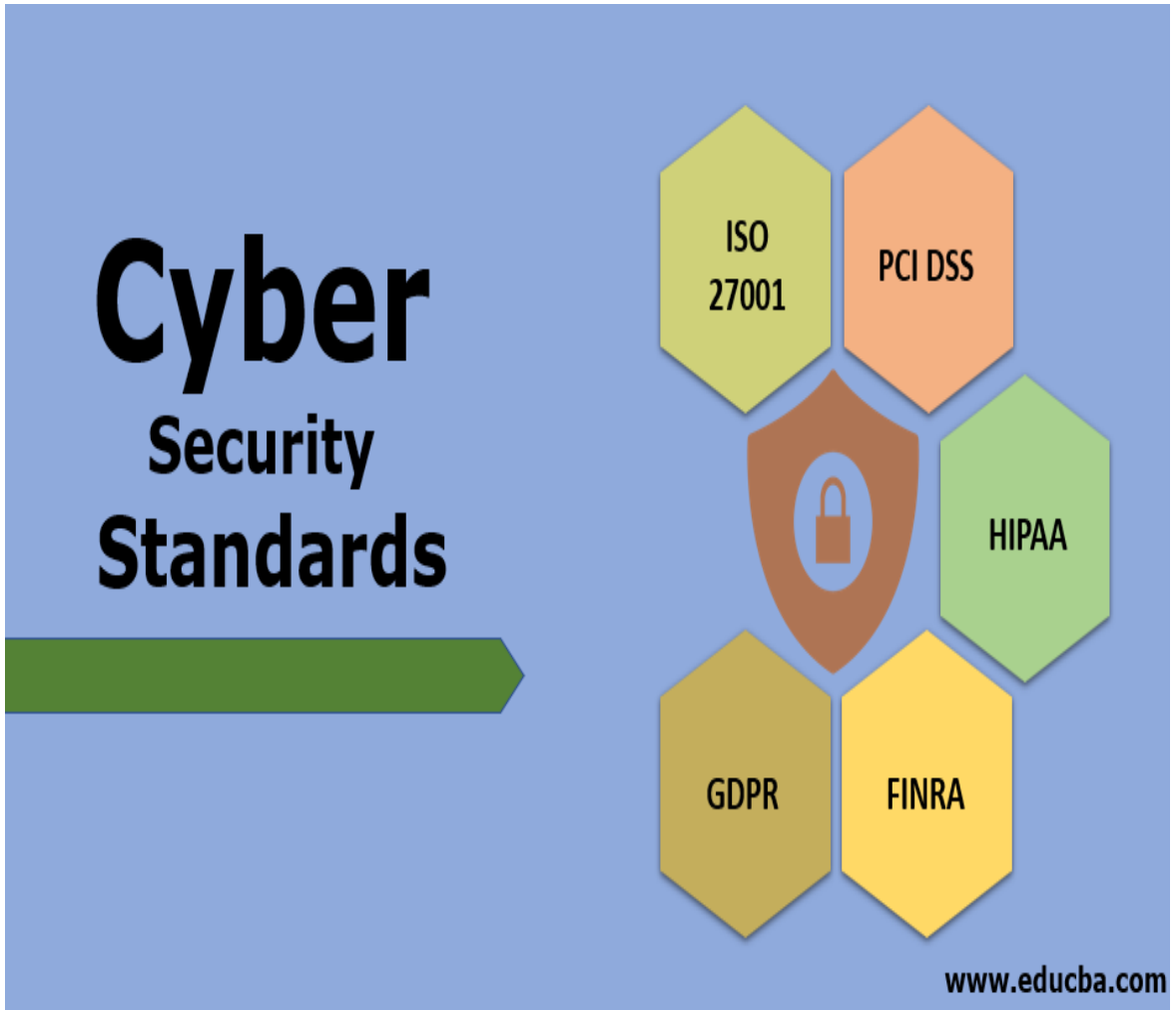
- Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyber attack. You can help protect yourself through education or a technology solution that filters malicious emails.
- See how a simple forged email can lead to a massive data breach and perhaps irreversible damage to an organisation's reputation.
  - https://www.youtube.com/watch?v=668mc-_kJBM
- Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

TYPES OF CYBERSECURITY THREATS

- Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.
- Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.
- Check Point has developed a site which shows in real time the attacks happening all over the world. This is the link:
  - https://threatmap.checkpoint.com/

HOW TO PROTECT YOURSELF FROM CYBERATTACKS

SECURITY STANDARDS



- ISO/IEC 27001: Is an international standard on how to manage information security. It details requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS)
- PCI DSS: Payment Card Industry Data Security Standard (US)
- HIPAA: Health Insurance Portability and Accountability Act (US)
- FINRA: The Financial Industry Regulatory Authority (US)
- GDPR: General Data Protection Regulation (EU)

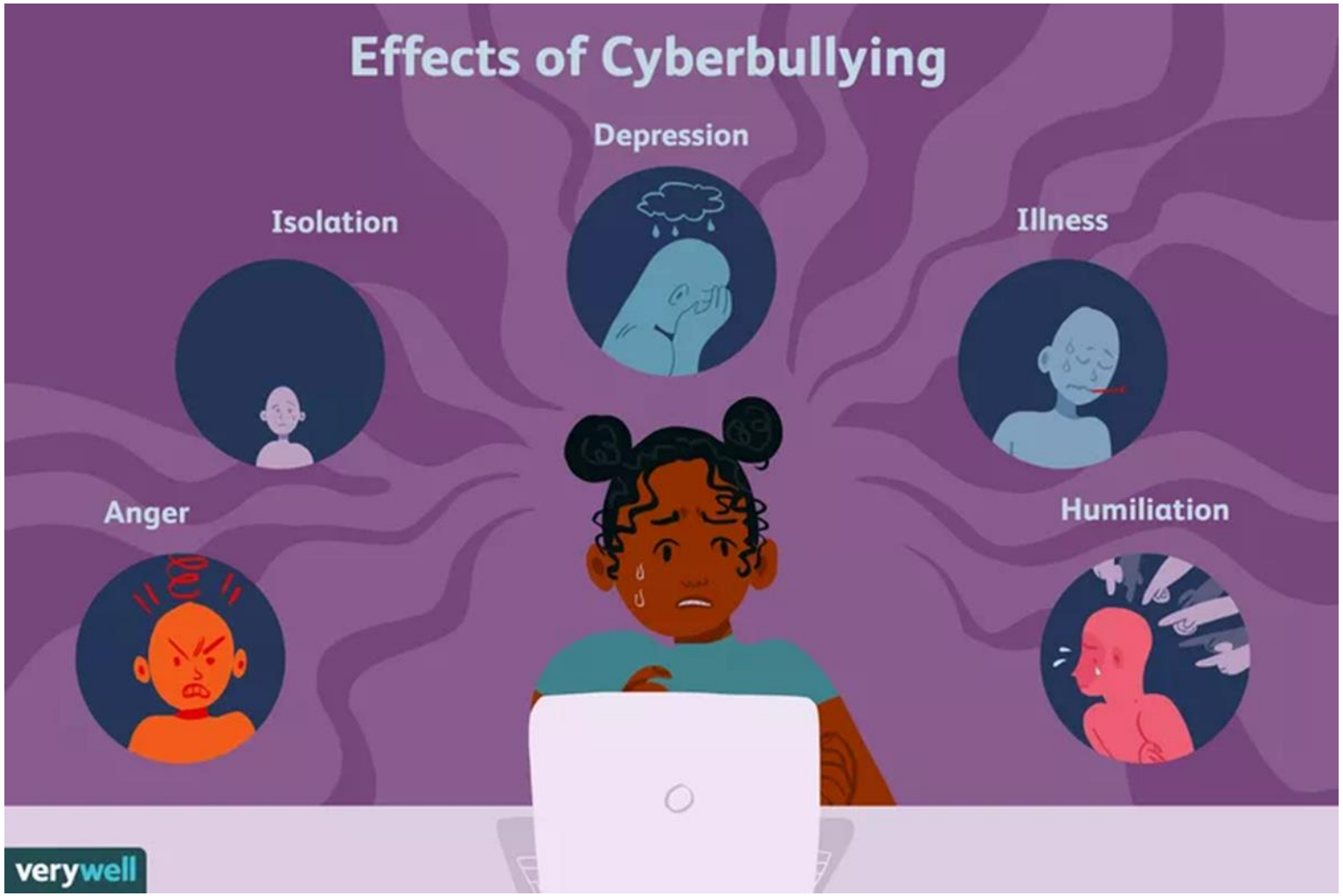
2. CYBERBULLYING

- Simply put, cyberbullying is when a child or teen becomes a target of actions by others – using computers, cellphones or other electronic devices – that are intended to embarrass, humiliate, threaten or harass. It can start as early as age eight or nine, but the majority of cyberbullying takes place in the teenage years, up to age 17.
- Kids call it hating, drama, gossip or trolling. Whatever name it goes by, cyberbullying is serious. It can be emotionally damaging and even lead to tragic consequences.
- Unlike face-to-face bullying, cyberbullying can be relentless. It can reach a victim anywhere at anytime.

UNDERSTANDING CYBERBULLYING

- Because it can spread quickly, to a wide audience, you might be surprised to learn that most teens today have been involved in some way or other, either as a target, as a bully, as a silent observer, or as someone who participates on the sidelines and becomes part of the problem without realizing what they're doing.
- Most often, it's sustained and repeated over a period of time. But whether it's sharing one humiliating photo or 1,000 harmful text messages, it can damage a young person's feelings, self-esteem, reputation and mental health.

EFFECTS OF CYBERBULLYING



CYBERBULLYING TACTICS

- The range of cyberbullying tactics is wide and is continually changing as new technology emerges and different social networking sites pop up.
- Here are some of the common ways that cyberbullying is taking place among young people:
  - Sending mean or threatening messages by email, text or through comments on a social networking page.
  - Spreading embarrassing rumors, secrets or gossip about another person through social networking sites, email, or texts.
  - Taking an embarrassing picture or video of someone with a digital camera and sending it to others or posting it online without their knowledge or permission.

CYBERBULLYING TACTICS

- Posting online stories, pictures, jokes, or cartoons that are intended to embarrass or humiliate.
- Hacking someone's email account and sending hurtful content to others while pretending to be them.
- Using someone else's password to get into their social networking account and post material as them that would be embarrassing or offensive.
- Tricking someone to open-up and share personal information and then sharing that information widely with others.

CYBERBULLYING STATISTICS

- In a 2019 study of a nationally-representative sample of approximately 5,000 middle and high schoolers in the U.S.:
  - 36.5% said they had been cyberbullied during their lifetime.
  - 17.4% said they had been cyberbullied within the previous 30 days.
  - With regard to offending, 14.8% revealed they had cyberbullied others during their lifetime, while 6.3% admitted doing so in the last 30 days.

CYBERBULLYING VS TRADITIONAL BULLYING

- With cyberbullying, targets may not know who is targeting them, or why. The aggressor can cloak his or her identity using anonymous accounts and pseudonymous screennames.
- The hurtful actions of those who cyberbully can more easily go viral; that is, a large number of people (at school, in the neighborhood, in the city, in the world!) can participate in the victimization.
- It is often easier to be cruel using technology because cyberbullying can be done from a physically distant location. In fact, some teens simply might not realize the serious harm they are causing because they are sheltered from the target's response.
- Finally, while parents and teachers are doing a better job monitoring youth at school and at home, many adults don't have the technological know-how (or time) to keep track of what teens are up to online.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

OBSTACLES

- Even though this problem has been around for over two decades, some people still don't see the harm associated with it. We first need to accept that cyberbullying is a problem that will only get worse if ignored.
- Parents often say that they don't have the knowledge or time to keep up with their children's online behavior, and that schools should be covering it in detail during class time and through other programming.
- Educators are often doing their part through policies, curricula, training, and assemblies, but sometimes don't know when and how to intervene in online behaviors that occur away from school but still involve their students.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

OBSTACLES

- Law enforcement is hesitant to get involved unless there is clear evidence of a crime or a significant threat to someone's physical safety.
- We need to get everyone involved - youth, parents, educators, counselors, youth leaders, law enforcement, social media companies, and the community at large.
- It takes concerted and comprehensive effort from all stakeholders to make a meaningful difference in reducing cyberbullying.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF PARENTS

- Parents should make sure when their child is cyberbullied that he/she feels safe, and to convey unconditional support.
- Parents may also be able to contact the parents of the aggressor, school, Internet Service Provider, to investigate the issue or remove the offending material.
- Parents must educate their children about appropriate online behaviors just as they convey appropriate offline behaviors. They should also monitor their child's activities while online – especially early in their exploration of cyberspace.
- Youth need to learn that inappropriate online actions will not be tolerated.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF PARENTS

- It is crucial that parents cultivate and maintain an open, candid line of communication with their children, so that they are inclined to reach out when they experience something unpleasant or distressing online.
- If a parent discovers that their child is cyberbullying others, they should first communicate how that behavior inflicts harm and causes pain in the real world.
- Consequences should be firmly applied depending on seriousness and intentionality (and escalated if the behavior continues).

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF SCHOOL

- The most important preventive step that schools can take is to educate their community about responsible use of their devices at all times.
- Students need to know that all forms of bullying are wrong and that those who engage in harassing or threatening behaviors will be subject to discipline.
- These messages should be reinforced in classes that regularly utilize technology. Posted rules around campus to remind students of acceptable use.
- It is crucial to establish and reinforce an environment of respect and integrity where violations result in informal or formal sanction.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF SCHOOL

- School personnel should review their harassment and bullying policies to ensure that it allows for the discipline of students who engage in cyberbullying.
- In some cases, simply discussing the incident with the offender's parents will result in the behavior stopping. If inappropriate behaviors continue, additional steps need to be taken.
- It is critical for educators to develop and promote a safe and respectful school climate.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF YOUTH

- Youth should develop a relationship with an adult they trust (a parent, teacher, or someone else) so they can talk about any experiences they have online (or off) that make them upset or uncomfortable.
- If possible, teens should ignore minor teasing or name calling, and not respond to the aggressor as that might simply make the problem continue.
- Youth should also use the account and privacy settings within each device, app, or network to control who can contact and interact with them, and who can read their online content. This can significantly reduce their victimization risk.
- It's useful to keep all evidence of cyberbullying to show an adult who can help. This could also greatly help during an investigation. This information can be forwarded to the respective site or company involved.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF YOUTH

- Youth should take the time to report any harassment, threats, impersonation, or other problems they see or experience, and remember that their identity will be protected to the maximum extent of the law when doing so.
- Youth should go online with their parents; show them what sites and apps they use. They should tell their parents how they are keeping themselves safe online and allow mom or dad to suggest other strategies as well.
- Finally, youth should pause before they post—and make wise decisions with what they share or send or post online, considering the possibility that anyone and everyone may see it.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF LAW ENFORCEMENT

- Law enforcement officers also have a role in preventing and responding to cyberbullying. They first need to be aware of ever-evolving state and local laws concerning online behaviors and equip themselves with the skills and knowledge to intervene as necessary.
- Even if the behavior doesn't appear to rise to the level of a crime, officers should use their discretion to handle the situation in a way that is appropriate for the circumstances. For example, a simple discussion of the legal issues involved in cyberbullying may be enough to deter some youth from future misbehavior.
- Officers might also talk to parents about their child's conduct and express to them the seriousness of online harassment.

ACTIONS TO MINIMIZE OR STOP CYBERBULLYING

THE ROLE OF LAW ENFORCEMENT

- Officers can play an essential role in preventing cyberbullying from occurring or getting out of hand in the first place. They can speak to students about cyberbullying and online safety issues more broadly to discourage them from engaging in risky or unacceptable actions and interactions.
- They might also address parents about local and state laws, so that they are informed and can properly respond if their child is involved in an incident.

"Unless and until our society recognizes cyber bullying for what it is, the suffering of thousands of silent victims will continue" - Anna María Chavez (Attorney)

Thank you!