BGD e-GOV CIRT

Cybersecurity For Kids

Cybersecurity for KIDS

WHAT IS CYBER SECURITY?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

WHAT IS INTERNET SECURITY?

★ Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

★ In today's digital landscape, many of our daily activities rely on the internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online. This means that tons of data and sensitive information are constantly being shared over the internet. The internet is mostly private and secure, but it can also be an insecure channel for exchanging information. With a high risk of intrusion by hackers and cybercriminals, internet security is a top priority for individuals and businesses alike.

Threats Internet Security

VIRUS Perhaps the most well-known computer security threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process.

HACKERS AND PREDATORS People, not computers, create computer security threats and malware. Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change, or destroy information as a form of cyber-terrorism. These online predators can compromise credit card information, lock you out of your data, and steal your identity. As you may have guessed, online security tools with identity theft protection are one of the most effective ways to protect yourself from this brand of cybercriminal.

PHISHING Masquerading as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing attacks are some of the most successful methods for cybercriminals looking to pull off a data breach.

CYBER PREDATORS	CYBERBULLYING
PRIVATE INFORMATION	SEXTING
OVEREXPOSING SOCIAL NETWORK	PHISHING

Cyber Predators

- The Internet is much more anonymous than the real world. People can hide their identities or even pretend to be someone they're not. This can sometimes present a real danger to children and teens who are online. Online predators may try to lure kids and teens into sexual conversations or even face-to-face meetings. Predators will sometimes send obscene material or request that kids send pictures of themselves. Therefore, it's important to teach your kids to be on their guard whenever they're online.

- Teens are generally more at risk from predators. Because they are curious and want to be accepted, they may talk to a predator willingly, even if they know it's dangerous. Sometimes teens may believe they are in love with someone online, making them more likely to agree to a face-to-face meeting.

- While it's not necessarily likely that your child will be contacted by a predator, the danger does exist. Below are some guidelines you can tell your kids to help them stay safe from online predators.

- Don't talk to anyone who wants to get too personal. If they want to talk about things that are sexual or personal, you should end the conversation. Once you get pulled into a conversation (or a relationship).

- Avoid using suggestive screen names or photos. These can result in unwanted attention from online predators.

- If someone is flattering you online, you should be wary. Although many people online are genuinely nice, predators may use flattery to try to start a relationship with a teen. This doesn't mean you need to be suspicious of everyone, but you should be careful.

- Keep in mind that people are not always who they say they are. Predators may pretend to be children or teenagers to talk to kids online. They may use a fake profile picture and add other profile details to appear more convincing.

Cyberbullying

Just as predators no longer have to leave their homes to interact with children, bullies no longer have to be face to face with their victims. Cyberbullying through social media sites is unfortunately prevalent in today's world and causes just as much damage as any other form of bullying. This is arguably one of the most challenging threats to deal with, though a solution is to prevent your children from creating social media profiles in the first place. Let them know they can create theirs when they're older. If you don't want to do this, remind your children that they can always come to you if they're being bullied, whether online or not. You won't be able to do much unless you know it's happening in the first place.

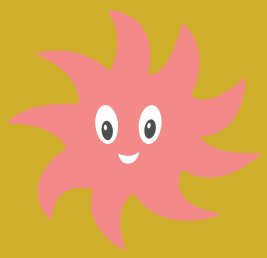
The vast majority, 90%, of teens agree that cyber bullying a problem, and 63% believe this is a serious problem. What's more, a 2018 survey of children's online behavior found that approximately 60% of children who use social media have witnessed some form of bullying, and that, for various reasons, most children ignored the behavior altogether. And according to enough.org, as of February 2018, nearly half (47%) of all young people had been the victims of cyber bullying. Social media and online games are today's virtual playground, and that is where much cyber bullying takes place, and it's operating 24/7. Children can be ridiculed in social media exchanges. Or, in online gaming, their player personas can be subjected to incessant attack, turning the game from an imaginative adventure into a humiliating ordeal that escalate into cyber bullying across multiple platforms and in real-life.

The best foundation for protecting against cyber bullying is to be comfortable talking to your children about what is going on in their lives online and in in real-life (IRL) and how to stand up to bullies. Cyber security software and specialized apps for monitoring your child's online and mobile activity can help, but nothing will replace an open dialog.

BGD e-GOV CIRT

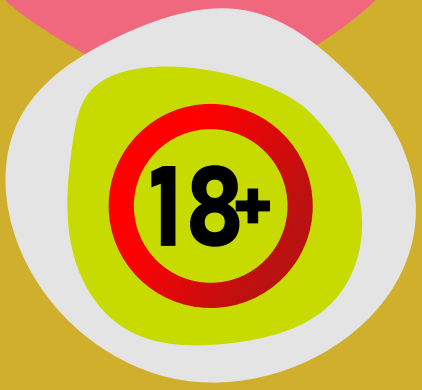
Private Information

Children do not yet understand social boundaries. They may post personally identifiable information (PII) online, for example in their social media profiles, that should not be out in public. This might be anything from images of awkward personal moments to their home addresses or family vacation plans.



Much, but not all, of what your children post is in public view. This means that you can also see it—and there's no harm in reminding them that if Mom and Dad can see it, so can everyone else. Avoid snooping, but speak frankly to your kids about public boundaries and what they mean for your children and your family as a whole.

SEXTING



Sexting is sending sexually explicit messages, photos, or videos via cell phone, computer, or any digital device. Sexting includes photos and videos containing nudity or showing simulated sex acts. It also includes text messages that discuss or propose sex acts.

As teens and children increasingly carry smartphones and use tablets, social media, apps, and messaging, the risks that they will send or receive sexually explicit content has become a concern for parents, teachers, and law enforcement.

Sexting is often done as a joke, a way of getting attention, or as flirting. Parents should discuss the issue with their children to ensure they understand the risks and what to if or when they're pressured to participate.

SEXTING

Why Is Sexting a Problem?

A photo shared between two people can quickly become a viral phenomenon. Teens may believe it will be kept private and then discover it has been shared widely with their peers, sometimes with grave consequences. These include arrests of teens who shared photos of themselves or other underage teens.

While some states have laws that differentiate sexting from child pornography, others do not. Sexting could result in charges of distributing or possessing child pornography.

Bullying, harassment, and humiliation are common problems when the photos and messages get shared beyond the intended recipient. There can be severe emotional and social consequences, including suicides of teens who had their photos shared.

How Can Parents Prevent Sexting?

Start the conversation before your child has an incident. If you are giving your child a smartphone or webcam, that is the time to talk about sexting. You also can use news stories or plotlines in television shows or movies as a conversation starter.

The best approach to talking about sexting is to take a non-judgmental and informational one. Keeping the dialogue open leaves room for your kids to talk with you rather than hiding things away. Also, be aware that kids may have a different name for sexting, so you'll need to be clear about the topic you are discussing.

Overexposing Social Network

If we are more and more willing to expose our lives on social networking sites and share all kinds of moments and situations, we don't necessarily need to abandon caution to think and choose what to publish, where to publish and, especially, for whom to publish. Overexposure, known worldwide as Oversharing, is difficult to measure, but we can always start with common sense and a reflection on the context in which we share something.

We are all free to share things in our lives with others, but we cannot forget the differences of exposure on and off the web. If on a bus or plane trip, or even in a bank line, we don't feel comfortable sharing and exposing part of our intimacy with strangers, then we know that it's not all kinds of content that we can expose, both for our safety and so as not to embarrass the other person.

On the Internet, the same care must be taken, added to some important differences because everything, everything we share is registered and we lose full control over who can have access to this content. We are no longer the only owners of information that can be used not just by the sites that host the sites and services, but by users all over the world who can search and find these details about our lives very easily if we overindulge in online exposure. And, as always, information about our intimacy taken out of context can hurt us, both now and in the future.

BGD e-GOV CIRT

PHISHING

Phishing is what cyber security professionals call the use of emails that try to trick people into clicking on malicious links or attachments. These can be especially difficult for kids to detect because often, the email will appear to be from someone legitimate, like a friend or family member, saying simply, "Hey— thought you might like this!" This can also be done with using messaging apps or text messages—then it's called "smishing". (Smishing is an attack that uses text messaging or short message service (SMS) to execute the attack. A common smishing technique is to deliver a message to a cell phone through SMS that contains a clickable link or a return phone number.)

Email Phishing

The basic phishing email is sent by fraudsters impersonating legitimate companies, often banks or credit card providers. These emails are designed to trick you into providing log-in information or financial information, such as credit card numbers or Social Security numbers.

Spear Phishing

While most phishing emails are sent to large groups of people, there is one type of attack that is more personalized in nature, spear phishing.

Spear-phishing emails are targeted toward a specific individual, business or organization. And unlike more generic phishing emails, the scammers who send them spend time researching their targets.

Clone Phishing

Another type of phishing, clone phishing, might be one of the most difficult to detect. In this type of phishing attack, scammers create a nearly identical version of an email that victims have already received.

The cloned email is sent from an address that is nearly, but not quite, the same as the email address used by the message's original sender.

BGD e-GOV CIRT

BGD e-GOV CIRT

CYBERSECURITY FOR KIDS