Cyber security for kids

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos

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. (EN-USA)
- Segurança cibernética é a prática de defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. É também conhecido como segurança da tecnologia da informação ou segurança da informação eletrônica. O termo se aplica a uma variedade de contextos, de negócios a computação móvel, e pode ser dividido em algumas categorias comuns. (PT-BR)

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

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.
- A segurança na Internet consiste em uma variedade de táticas de segurança para proteger atividades e transações realizadas online pela Internet. Essas táticas têm como objetivo proteger os usuários de ameaças como invasão de sistemas de computador, endereços de e-mail ou sites; software malicioso que pode infectar e danificar sistemas inerentemente; e roubo de identidade por hackers que roubam dados pessoais, como informações de contas bancárias e números de cartão de crédito. A segurança da Internet é um aspecto específico de conceitos mais amplos, como a segurança cibernética e a segurança do computador, com foco nas ameaças e vulnerabilidades específicas do acesso online e do uso da Internet.
- No cenário digital de hoje, muitas de nossas atividades diárias dependem da internet. Várias formas de comunicação, entretenimento e tarefas financeiras e de trabalho são realizadas online. Isso significa que toneladas de dados e informações confidenciais são constantemente compartilhados pela Internet. A Internet é principalmente privada e segura, mas também pode ser um canal inseguro para a troca de informações. Com um alto risco de invasão por hackers e cibercriminosos, a segurança da Internet é uma prioridade para indivíduos e empresas.

https://www.mcafee.com/enterprise/pt-br/security-awareness/cybersecurity/what-is-internet-security.html

Threats Internet Security

- Vírus: 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.
- Vírus: Talvez a mais conhecida ameaça à segurança de computador, um vírus de computador é um programa criado para alterar o funcionamento de um computador, sem a permissão ou conhecimento do usuário. Um vírus se replica e executa a si mesmo, geralmente causando danos ao computador durante o processo.
- Hackers e predadores: pessoas, não computadores, criam malware e ameaças à segurança do computador. Hackers e predadores são programadores que vitimam outras pessoas para seu próprio ganho, invadindo sistemas de computador para roubar, alterar ou destruir informações como uma forma de terrorismo cibernético. Esses predadores online podem comprometer as informações do cartão de crédito, bloquear seus dados e roubar sua identidade. Como você deve ter adivinhado, as ferramentas de segurança online com proteção contra roubo de identidade são uma das maneiras mais eficazes de se proteger dessa marca de cibercriminoso.
- Phishing: mascarando-se como uma pessoa ou empresa confiável, os phishers tentam roubar informações pessoais ou financeiras confidenciais por meio de e-mail fraudulento ou mensagens instantâneas. Ataques de phishing são alguns dos métodos de maior sucesso para os cibercriminosos que buscam uma violação de dados.

https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats

Cyber Predators

Threats Internet Security Kids

- 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.
- **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.
- **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), it may be more difficult to stop.
- **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.
- **Never arrange to meet with someone you met online.** Predators may try to arrange a face-to-face meeting with a child or teen. Even if the person seems nice, this can be dangerous.
- **Tell a parent or trusted adult if you encounter a problem.** If anyone makes you feel uncomfortable online, you should tell a parent or trusted adult immediately. You should also save any emails or other communication because they may be needed as evidence.

Threats Internet Security Kids

- A Internet é muito mais anônima do que o mundo real. As pessoas podem esconder suas identidades ou até fingir ser alguém que não são. Às vezes, isso pode representar um perigo real para crianças e adolescentes que estão online. Predadores online podem tentar atrair crianças e adolescentes para conversas sexuais ou mesmo encontros cara a cara. Predadores às vezes enviam material obsceno ou solicitam que as crianças enviem fotos de si mesmas. Portanto, é importante ensinar seus filhos a ficarem alertas sempre que estiverem online.
- Os adolescentes geralmente correm mais risco de predadores. Por serem curiosos e quererem ser aceitos, eles podem falar com um predador de boa vontade, mesmo que saibam que é perigoso. Às vezes, os adolescentes podem acreditar que estão apaixonados por alguém online, o que os torna mais propensos a concordar em um encontro cara a cara.
- Embora não seja necessariamente provável que seu filho seja contatado por um predador, o perigo existe. Abaixo estão algumas diretrizes que você pode dizer a seus filhos para ajudá-los a se protegerem de predadores online.
- Evite usar nomes de tela ou fotos sugestivos. Isso pode resultar em atenção indesejada de predadores online.
- Se alguém está elogiando você online, você deve ser cauteloso. Embora muitas pessoas online sejam genuinamente legais, os predadores podem usar a bajulação para tentar iniciar um relacionamento com um adolescente. Isso não significa que você precise suspeitar de todos, mas deve ter cuidado.
- Não fale com ninguém que queira se tornar muito pessoal. Se eles quiserem falar sobre coisas sexuais ou pessoais, você deve encerrar a conversa. Depois de ser puxado para uma conversa (ou relacionamento), pode ser mais difícil parar.
- Lembre-se de que as pessoas nem sempre são quem dizem ser. Predadores podem fingir ser crianças ou adolescentes para falar com as crianças online. Eles podem usar uma foto de perfil falsa e adicionar outros detalhes de perfil para parecer mais convincente.
- Nunca combine um encontro com alguém que conheceu online. Os predadores podem tentar marcar um encontro cara a cara com uma criança ou adolescente. Mesmo que a pessoa pareça legal, isso pode ser perigoso.
- Diga a seus pais ou adulto de confiança se encontrar um problema. Se alguém fizer você se sentir desconfortável online, informe imediatamente a seus pais ou a um adulto de confiança. Você também deve salvar todos os e-mails ou outras comunicações porque podem ser necessários como prova.

Threats Internet Security Kids

- **Who to contact if there's a problem**
- If you think your child is being contacted by an online predator, seek immediate help from the following resources:
- **Local police:** If your child is in immediate danger, you should call **911**. Otherwise, you can call your local police's non-emergency number to report a problem.
- Digital means of reporting a crime on the internet if the local police do not have enough resources, such as police stations specializing in cybercrime

Threats Internet Security Kids

- **Quem contatar se houver um problema**
- Se você acha que seu filho está sendo contatado por um predador online, procure ajuda imediata nos seguintes recursos:
- Polícia local: Se seu filho estiver em perigo imediato, você deve ligar para o 911. Caso contrário, você pode ligar para o número não emergencial da polícia local para relatar um problema.
- Meio digital de denunciar um crime na internet, se a polícia local não tiver recursos suficientes, como delegacias especializadas em crimes cibernéticos

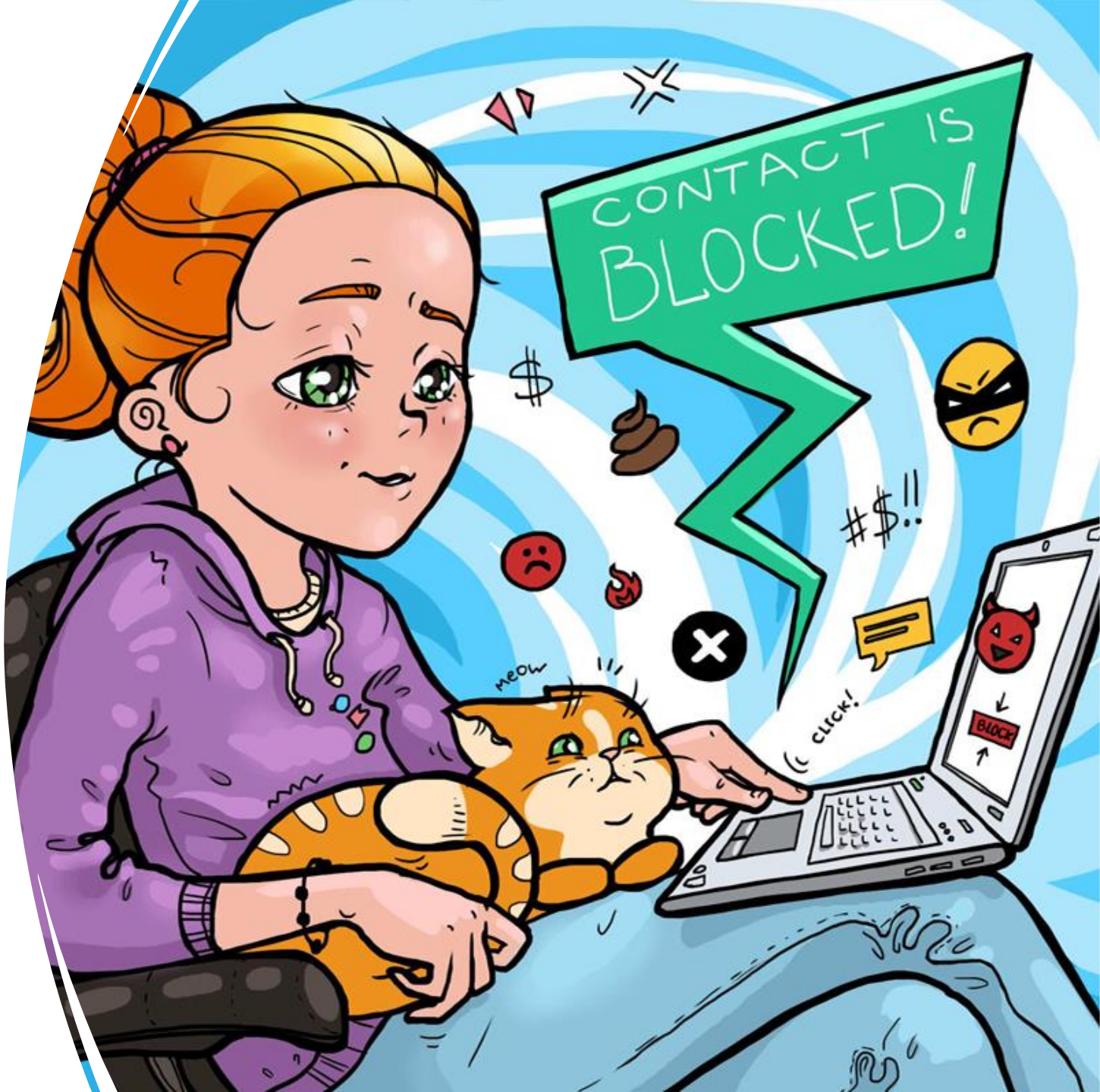
Threats Internet Security Kids – Cyberpredator Content

- https://www.youtube.com/watch?v=6jMhMVEjEQg&
- https://www.youtube.com/watch?v=DFWjf5_O-fk
- https://www.youtube.com/watch?v=euc-WcN5IkY&t
- https://www.youtube.com/watch?v=dbg4hNHsc_8
- https://www.youtube.com/watch?v=xk4VmYrquAs
- https://www.youtube.com/watch?v=m6Z7EWFTYTU&t

Cyberbullying

Threats Internet Security Kids – 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.

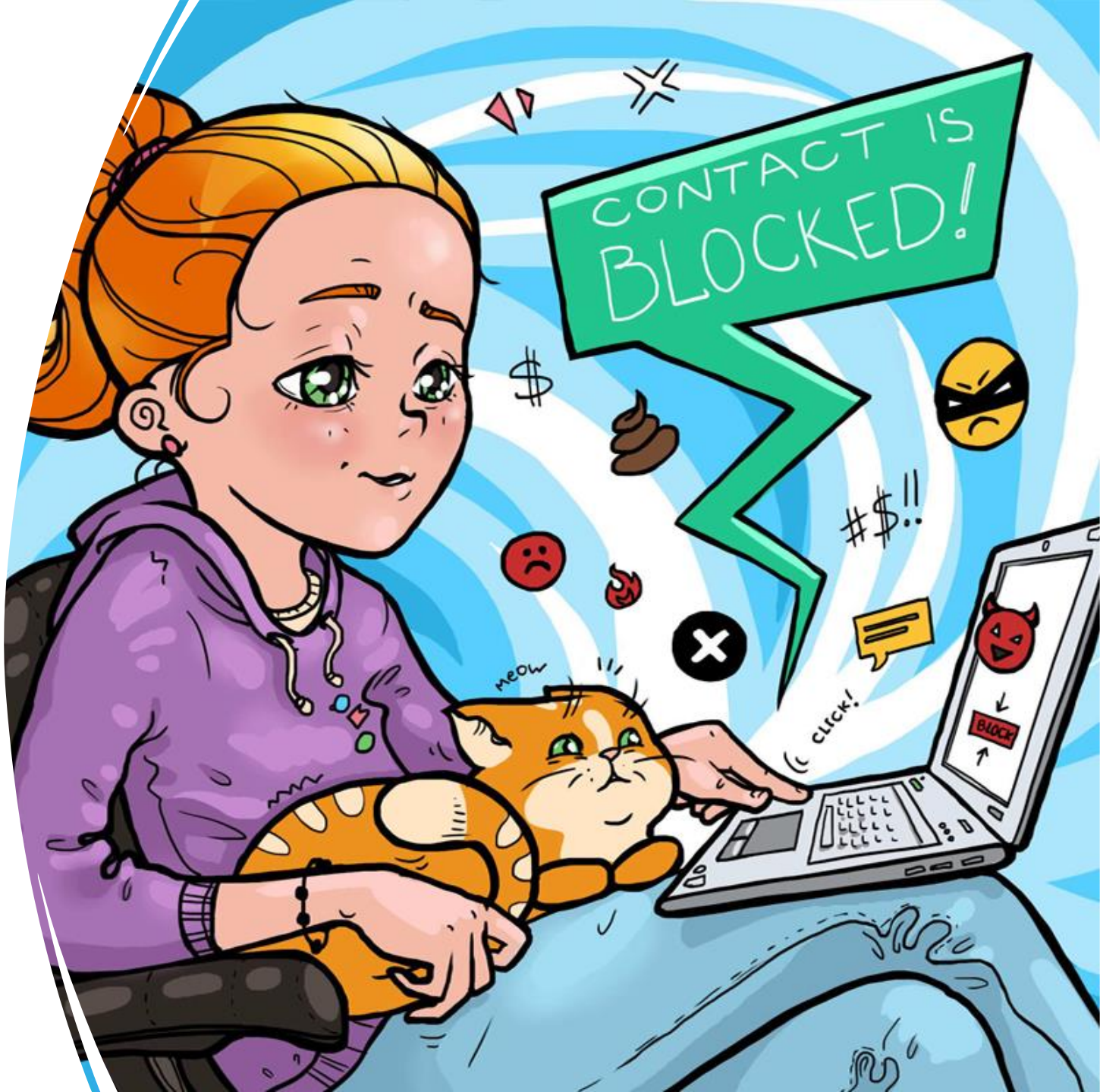


Threats Internet Security Kids – Cyberbullying

- Assim como os predadores não precisam mais deixar suas casas para interagir com as crianças, os agressores não precisam mais ficar cara a cara com suas vítimas. O cyberbullying por meio de sites de mídia social infelizmente prevalece no mundo de hoje e causa tantos danos quanto qualquer outra forma de bullying. Esta é sem dúvida uma das ameaças mais desafiadoras de se lidar, embora a solução seja evitar que seus filhos criem perfis de mídia social em primeiro lugar. Deixe-os saber que podem criar os seus quando forem mais velhos. Se você não quiser fazer isso, lembre seus filhos que eles sempre podem ir até você se estiverem sofrendo bullying, seja online ou não. Você não será capaz de fazer muito a menos que saiba que está acontecendo em primeiro lugar.

- A grande maioria, 90%, dos adolescentes concorda que o cyberbullying é um problema e 63% acreditam que este é um problema sério. Além do mais, uma pesquisa de 2018 sobre o comportamento on-line de crianças descobriu que aproximadamente 60% das crianças que usam as mídias sociais testemunharam alguma forma de bullying e que, por vários motivos, a maioria das crianças ignorou o comportamento por completo. E de acordo com o enough.org, em fevereiro de 2018, quase metade (47%) de todos os jovens foram vítimas de cyber bullying. A mídia social e os jogos online são o playground virtual de hoje, e é aí que ocorre grande parte do cyber bullying, funcionando 24 horas por dia, 7 dias por semana. As crianças podem ser ridicularizadas nas trocas de mídia social. Ou, em jogos online, suas personas de jogador podem ser submetidas a ataques incessantes, transformando o jogo de uma aventura imaginativa em uma provação humilhante que se transforma em cyber bullying em várias plataformas e na vida real.

- A melhor base para se proteger contra o cyber bullying é sentir-se à vontade para conversar com seus filhos sobre o que está acontecendo em suas vidas online e na vida real (IRL) e como enfrentá-los. Software de segurança cibernética e aplicativos especializados para monitorar a atividade on-line e móvel do seu filho podem ajudar, mas nada substituirá um diálogo aberto.



Threats Internet Security Kids – Cyberbullying Content

- https://www.youtube.com/watch?v=mWQoikd72A4
- https://www.youtube.com/watch?v=f6K9Ie_Chjs
- https://www.youtube.com/watch?v=pHtnr7wkN7E
- https://www.youtube.com/watch?v=Y9D2PFD7nTI
- https://www.youtube.com/watch?v=E0WbSOpIlgY
- https://www.youtube.com/watch?v=eQo-TknxI_I
- https://www.youtube.com/watch?v=asTti6y39xI
- https://www.youtube.com/watch?v=LC1BYXkHG3A
- https://www.youtube.com/watch?v=GsE6spm-gyI
- https://www.youtube.com/watch?v=xAk8FqRFXY0
- https://www.youtube.com/watch?v=Ne9rPuoNi9w
- https://www.youtube.com/watch?v=vmQ8nM7b6XQ
- https://www.youtube.com/watch?v=i1oF5pXq2bc
- https://www.youtube.com/watch?v=_t8Lf_hcuJk
- https://www.youtube.com/watch?v=CZ0YzebcBxw

Private Information

Threats Internet Security Kids – 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.

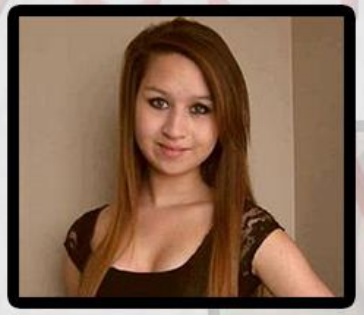
Threats Internet Security Kids – Private Information

- As crianças ainda não entendem as fronteiras sociais. Eles podem publicar informações de identificação pessoal (PII) online, por exemplo, em seus perfis de mídia social, que não devem ser divulgadas publicamente. Isso pode ser qualquer coisa, desde imagens de momentos pessoais embaraçosos até os endereços de suas casas ou planos de férias com a família.
- Muito, mas não tudo, o que seus filhos postam está à vista do público. Isso significa que você também pode ver - e não há mal nenhum em lembrá-los de que, se mamãe e papai podem ver, todo mundo também pode. Evite bisbilhotar, mas fale francamente com seus filhos sobre os limites públicos e o que eles significam para eles e sua família como um todo.

Threats Internet Security Kids – Private Information Content

- https://www.youtube.com/watch?v=opRMrEfAIiI
- https://www.youtube.com/watch?v=TyVM-H9P1RI
- https://www.youtube.com/watch?v=9XebSJxJYuo
- https://www.youtube.com/watch?v=1DmoMR-oX6o
- https://www.youtube.com/watch?v=yYFOCKq8WA4
- https://www.youtube.com/watch?v=PIlMsykXqLk

Cyber Bullying Victims



Amanda Todd
1996-2012

Phoebe Prince
1994-2010

Ryan Halligan
1989-2003

Tyler Clementi
1991-2010

Megan Meier
1992-2006

www.nobullying.com

Sexting

Threats Internet Security Kids – 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.1
- 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.

Threats Internet Security Kids – Sexting

- Sexting é o envio de mensagens, fotos ou vídeos sexualmente explícitos por meio de telefone celular, computador ou qualquer dispositivo digital. Sexting inclui fotos e vídeos contendo nudez ou mostrando atos sexuais simulados. Também inclui mensagens de texto que discutem ou propõem atos sexuais.
- À medida que adolescentes e crianças carregam cada vez mais smartphones e usam tablets, mídias sociais, aplicativos e mensagens, os riscos de enviarem ou receberem conteúdo sexualmente explícito se tornou uma preocupação para pais, professores e policiais. [1]
- O sexting costuma ser feito como uma piada, uma forma de chamar a atenção ou como um flerte. Os pais devem discutir o assunto com seus filhos para garantir que eles entendam os riscos e o que fazer se ou quando forem pressionados a participar.

Threats Internet Security Kids – 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.2
- 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.

Threats Internet Security Kids – Sexting

- **Por que o sexting é um problema?**
- Uma foto compartilhada entre duas pessoas pode rapidamente se tornar um fenômeno viral. Os adolescentes podem acreditar que será mantido em sigilo e, então, descobrir que foi amplamente compartilhado com seus colegas, às vezes com consequências graves. Isso inclui prisões de adolescentes que compartilharam fotos suas ou de outros adolescentes menores de idade.
- Embora alguns estados tenham leis que diferenciam o sexo da pornografia infantil, outros não. Sexting pode resultar em acusações de distribuição ou posse de pornografia infantil.
- Intimidação , assédio e humilhação são problemas comuns quando as fotos e mensagens são compartilhadas além do destinatário pretendido. Pode haver graves consequências emocionais e sociais, incluindo suicídios de adolescentes que tiveram suas fotos compartilhadas.

Threats Internet Security Kids – Sexting

- **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.

Threats Internet Security Kids – Sexting

- **Como os pais podem prevenir o sexting?**
- Comece a conversa antes que seu filho tenha um incidente. Se você está dando a seu filho um smartphone ou webcam, é hora de falar sobre sexting. Você também pode usar notícias ou enredos em programas de televisão ou filmes para iniciar uma conversa.

- A melhor abordagem para falar sobre sexting é não fazer julgamentos e usar informações. Manter o diálogo aberto abre espaço para que seus filhos conversem com você, em vez de esconder as coisas. Além disso, esteja ciente de que as crianças podem ter um nome diferente para sexting, então você precisa ser claro sobre o assunto que está discutindo.

Threats Internet Security Kids – Sexting Content

- https://www.youtube.com/watch?v=PL57cjJlp7g
- https://www.youtube.com/watch?v=MoRtLk1xihY
- https://www.youtube.com/watch?v=SuBxI5OGdlw
- https://www.youtube.com/watch?v=uFKAFo_etkE
- https://www.youtube.com/watch?v=RWxAimnKupE
- https://www.youtube.com/watch?v=UPgHh3wOusI
- https://www.youtube.com/watch?v=oAI2ajdDIrk
- https://www.verywellfamily.com/what-is-sexting-problem-1258921
- https://www.webmd.com/sex/what-is-sexting

Overexposing Social Network

Threats Internet Security Kids – 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.

Threats Internet Security Kids – Overexposing Social Network

- Se cada vez mais estamos dispostos a expor nossas vidas nos sites de redes sociais e compartilhar todo tipo de momento e situação, não obrigatoriamente precisamos abandonar a cautela para pensar e escolher o que publicar, onde publicar e, principalmente, para quem publicar. A Superexposição, conhecida mundialmente como Oversharing, é difícil de medir, mas podemos sempre partir do bom senso e de uma reflexão sobre o contexto no qual compartilhamos algo.
- Todos nós somos livres para poder compartilhar coisas de nossas vidas com os outros, mas não podemos nos esquecer das diferenças de uma exposição dentro e fora da rede. Se numa viagem de ônibus ou avião, ou até mesmo em uma fila de banco não nos sentimos a vontade para compartilhar e expor parte de nossa intimidade com estranhos, então sabemos que não é todo tipo de conteúdo que podemos expor, tanto para nossa segurança quanto para não causar constrangimento na outra pessoa.
- Na Internet deve valer o mesmo cuidado, somada a algumas diferenças importantes pois tudo, tudo o que compartilhamos fica registrado e perdemos o controle total sobre quem poderá ter acesso a este conteúdo. Deixamos de ser os únicos donos das informações que podem ser usadas não apenas pelos sites que hospedam os sites e serviços, mas pelos usuários do mundo todo que podem buscar e encontrar estes detalhes sobre nossa vida com muita facilidade se exageramos na exposição online. E, como sempre, informações sobre nossa intimidade usadas fora de contexto pode nos prejudicar, tanto no presente quanto o futuro.

Threats Internet Security Kids – Overexposing Social Network Content

- https://www.youtube.com/watch?v=0EFHbruKEmw
- https://www.youtube.com/watch?v=e2xm5fc5MQk
- https://www.youtube.com/watch?v=tRo9n8M7zIE
- https://www.youtube.com/watch?v=Zbqo7MGVElw&t
- https://www.youtube.com/watch?v=KdtPNRzuKrk
- https://www.youtube.com/watch?v=Y6oUf81b1OI
- https://www.youtube.com/watch?v=0hs8rc2u5ak
- https://www.youtube.com/watch?v=aP8yrkkLWlM&t

Phishing

Threats Internet Security Kids – 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.)

Threats Internet Security Kids – Phishing

- Phishing é o que os profissionais de segurança cibernética chamam de uso de e-mails que tentam induzir as pessoas a clicar em links ou anexos maliciosos. Isso pode ser especialmente difícil para as crianças detectar porque, muitas vezes, o e-mail parecerá ser de alguém legítimo, como um amigo ou membro da família, dizendo simplesmente: "Ei, achei que você gostaria disso!" Isso também pode ser feito usando aplicativos de mensagens ou mensagens de texto - então é chamado de "smishing". (Smishing é um ataque que usa mensagem de texto ou serviço de mensagens curtas (SMS) para executar o ataque. Uma técnica comum de smishing é enviar uma mensagem para um telefone celular por meio de SMS que contém um link clicável ou um número de telefone de retorno.)

Threats Internet Security Kids – Phishing

- **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.
- **Phishing de e-mail**
- O e-mail de phishing básico é enviado por fraudadores que se fazem passar por empresas legítimas, geralmente bancos ou operadoras de cartão de crédito. Esses e-mails têm o objetivo de induzir você a fornecer informações de login ou financeiras, como números de cartão de crédito ou CPF.

Threats Internet Security Kids – Phishing

- **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. The technique is sometimes called social engineering. These criminals will send emails that look like they’re from legitimate sources.
- **Spear phishing**
- Embora a maioria dos e-mails de phishing seja enviada a grandes grupos de pessoas, existe um tipo de ataque que é mais personalizado por natureza, o spear phishing.
- Os e-mails de spear-phishing são direcionados a um indivíduo, empresa ou organização específica. E, ao contrário de e-mails de phishing mais genéricos, os golpistas que os enviam passam tempo pesquisando seus alvos. A técnica às vezes é chamada de engenharia social. Esses criminosos enviarão e-mails que parecem ser de fontes legítimas.

Threats Internet Security Kids – Phishing

- **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. The body of the email looks the same, too. What's different? The attachment or link in the message has been changed. If victims click on those now, it will take them to a fake website or open an infected attachment.
- **Clone phishing**
- Outro tipo de phishing, o clone de phishing, pode ser um dos mais difíceis de detectar. Nesse tipo de ataque de phishing, os golpistas criam uma versão quase idêntica de um e-mail que as vítimas já receberam.
- O e-mail clonado é enviado de um endereço que é quase, mas não exatamente, o mesmo endereço de e-mail usado pelo remetente original da mensagem. O corpo do e-mail também parece o mesmo. O que é diferente? O anexo ou link da mensagem foi alterado. Se as vítimas clicarem neles agora, isso os levará a um site falso ou abrirá um anexo infectado.

Threats Internet Security Kids – Phishing

- **Whaling**
- Sometimes phishers go after the biggest of targets, the whales. Whaling attacks target chief executive officers, chief operating officers, or other high-ranking executives in a company. The goal is to trick these powerful people into giving up the most sensitive of corporate data.
- These attacks are more sophisticated than general phishing attacks and require plenty of research from scammers. They usually rely on fraudulent emails that appear to be from trusted sources within the company or from legitimate outside agencies.
- **Whaling**
- Às vezes, os phishers vão atrás do maior dos alvos, as baleias. Os ataques de caça às baleias têm como alvo CEOs, diretores de operações ou outros executivos de alto escalão de uma empresa. O objetivo é induzir essas pessoas poderosas a abrir mão dos dados corporativos mais confidenciais.
- Esses ataques são mais sofisticados do que os ataques de phishing em geral e exigem muita pesquisa de golpistas. Eles geralmente dependem de e-mails fraudulentos que parecem ser de fontes confiáveis dentro da empresa ou de agências externas legítimas.

Threats Internet Security Kids – Phishing

- **Pop-up phishing**
- Pop-up phishing is a scam in which pop-up ads trick users into installing malware on their computers or convince them to purchase antivirus protection they don’t need.
- These pop-up ads sometimes use scare tactics. A common pop-up phishing example is when an ad might pop up on a user’s screen warning the user that their computer has been infected and the only way to remove the virus is by installing a particular type of antivirus software.
- Once the user installs this software, it either doesn’t work or, worse, actually does infect the computer with malware.
- **Pop-up phishing**
- O phishing pop-up é um golpe no qual os anúncios pop-up enganam os usuários para que instalem malware em seus computadores ou os convença a adquirir uma proteção antivírus de que não precisam.
- Esses anúncios pop-up às vezes usam táticas de intimidação. Um exemplo comum de pop-up de phishing é quando um anúncio pode aparecer na tela de um usuário avisando-o de que seu computador foi infectado e que a única maneira de remover o vírus é instalando um tipo específico de software antivírus.
- Depois que o usuário instala esse software, ele não funciona ou, pior, infecta o computador com malware.

Threats Internet Security Kids – Phishing and Social Engineering Content

- https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html
- https://www.youtube.com/watch?v=WNVTGTrWcvw
- https://www.youtube.com/watch?v=JzoJeJBdhuI
- https://www.youtube.com/watch?v=Y7zNlEMDmI4
- https://www.youtube.com/watch?v=9TRR6lHviQc
- https://www.youtube.com/watch?v=BnmneAjVrM4&t
- https://www.youtube.com/watch?v=XsOWczwRVuc
- https://www.youtube.com/watch?v=j3nE8JQATXo
- https://www.youtube.com/watch?v=WG8V1_Sj5g0
- https://www.youtube.com/watch?v=_faMyjODoR0
- https://www.youtube.com/watch?v=6OHKRA8T18I
- https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them

Digital Footprinting

Threats Internet Security Kids – Digital Footprinting

- A digital footprint – sometimes called a digital shadow or an electronic footprint – refers to the trail of data you leave when using the internet. It includes websites you visit, emails you send, and information you submit online. A digital footprint can be used to track a person's online activities and devices. Internet users create their digital footprint either actively or passively.

What is a digital footprint?

- Whenever you use the internet, you leave behind a trail of information known as your digital footprint. A digital footprint grows in many ways – for example, posting on social media, subscribing to a newsletter, leaving an online review, or shopping online.
- Sometimes, it's not always obvious that you are contributing to your digital footprint. For example, websites can track your activity by installing cookies on your device, and apps can collate your data without you knowing it. Once you allow an organization to access your information, they could sell or share your data with third parties. Worse still, your personal information could be compromised as part of a data breach.
- You often hear the terms 'active' and 'passive' in relation to digital footprints:

Active digital footprints

- An active digital footprint is where the user has deliberately shared information about themselves – for example, through posting or participating on social networking sites or online forums. If a user is logged into a website through a registered username or profile, any posts they make form part of their active digital footprint. Other activities that contribute to active digital footprints include completing an online form – such as subscribing to a newsletter – or agreeing to accept cookies on your browser.

Passive digital footprints

- A passive digital footprint is created when information is collected about the user without them being aware that this is happening. For example, this occurs when websites collect information about how many times users visit, where they come from, and their IP address. This is a hidden process, which users may not realize is taking place. Other examples of passive footprints include social networking sites and advertisers using your likes, shares, and comments to profile you and target you with specific content.

Threats Internet Security Kids – Digital Footprinting

- Uma pegada digital - às vezes chamada de sombra digital ou pegada eletrônica - refere-se ao rastro de dados que você deixa ao usar a Internet. Inclui sites que você visita, e-mails que você envia e informações que você envia online. Uma pegada digital pode ser usada para rastrear as atividades e dispositivos online de uma pessoa. Os usuários da Internet criam sua pegada digital ativa ou passivamente.

O que é uma pegada digital?

- Sempre que você usa a Internet, você deixa um rastro de informações conhecido como pegada digital. A pegada digital cresce de várias maneiras - por exemplo, postando em mídias sociais, assinando um boletim informativo, deixando uma crítica online ou fazendo compras online.
- Às vezes, nem sempre é óbvio que você está contribuindo para sua pegada digital. Por exemplo, sites podem rastrear sua atividade instalando cookies em seu dispositivo, e aplicativos podem agrupar seus dados sem você saber. Depois de permitir que uma organização acesse suas informações, eles podem vender ou compartilhar seus dados com terceiros. Pior ainda, suas informações pessoais podem ser comprometidas como parte de uma violação de dados.
- Você costuma ouvir os termos 'ativo' e 'passivo' em relação às pegadas digitais:

Pegadas digitais ativas

- Uma pegada digital ativa é quando o usuário compartilha deliberadamente informações sobre si mesmo - por exemplo, por meio de postagem ou participação em sites de redes sociais ou fóruns online. Se um usuário estiver conectado a um site por meio de um nome de usuário ou perfil registrado, todas as postagens que ele fizer farão parte de sua pegada digital ativa. Outras atividades que contribuem para pegadas digitais ativas incluem o preenchimento de um formulário online - como assinar um boletim informativo - ou concordar em aceitar cookies em seu navegador.

Pegadas digitais passivas

- Uma pegada digital passiva é criada quando as informações sobre o usuário são coletadas, sem que ele perceba que isso está acontecendo. Por exemplo, isso ocorre quando os sites coletam informações sobre quantas vezes os usuários os visitam, de onde vêm e seus endereços IP. Este é um processo oculto, que os usuários podem não perceber que está ocorrendo. Outros exemplos de pegadas passivas incluem sites de redes sociais e anunciantes usando seus gostos, compartilhamentos e comentários para traçar seu perfil e direcioná-lo com conteúdo específico

Threats Internet Security Kids – Digital Footprinting Content

- https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint
- https://en.wikipedia.org/wiki/Digital_footprint
- https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints/
- https://www.internetsociety.org/learning/digital-footprints/
- https://learnenglishteens.britishcouncil.org/skills/reading/upper-intermediate-b2-reading/your-digital-footprint
- https://blog-reputationx-com.translate.goog/digital-footprint?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc
- https://techterms.com/definition/digital_footprint
- https://enhalo.co/360-security/detecting-the-hacker-digital-footprinting/

Tools Internet Security

Threats Internet Security Kids – Tool Internet Security

- https://www.jigsawacademy.com/the-top-5-cyber-security-tools-used-by-organizations/
- https://www.techtudo.com.br/tudo-sobre/pc-tools-internet-security.html
- https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/
- https://www.javatpoint.com/cyber-security-tools
- https://theexodusroad.com/10-tools-to-keep-your-kids-safe-online/
- https://staysafeonline.org/blog/guide-essential-tools-keep-children-safe-online/
- https://internetsafety101.org/Internetsafetytools
- https://www.makeuseof.com/tag/7-family-safety-tools-using-kids-online/
- https://www.yourlocalsecurity.com/blog/7-awesome-tech-tools-to-keep-kids-safe-online/
- https://www.kaspersky.com/resource-center/preemptive-safety/kids-online-safety
- https://kidshealth.org/en/parents/net-safety.html
- https://sectigostore.com/blog/internet-safety-for-kids-resources-tools-for-parents/
- https://br.norton.com/norton-family
- https://www.techradar.com/best/parental-control
- https://www.pcmag.com/picks/the-best-parental-control-software
- https://www.youtube.com/kids/parent-resources/

Extra Content

https://www.youtube.com/watch?v=JSx7MBIOnW4
https://www.csa.gov.sg/Programmes/sg-cyber-safe-students/videos/cyber-safety-kids-rsa-security
https://www.youtube.com/watch?v=8tR9P4QX82I
https://www.cisecurity.org/blog/6-educational-cybersecurity-resources-for-kids/
https://www.getcybersafe.gc.ca/en/blogs/cyber-security-kids-how-parents-can-talk-their-children
https://usa.kaspersky.com/resource-center/preemptive-safety/cybersecurity-for-kids
https://www.cisa.gov/sites/default/files/publications/Kids%20Cybersecurity%20Presentation.pdf
https://au.norton.com/internetsecurity-kids-safety-middle-school-kit-a-broader-world-of-cybersecurity-protection.html
https://www.safewise.com/resources/internet-safety-kids/
https://www.outlookindia.com/website/story/outlook-spotlight-cybersecurity-for-kids-its-never-too-early-to-begin/386647
https://www.triptecnologia.com.br/single-post/2019/10/11/10-dicas-de-seguran%C3%A7a-na-internet-para-crian%C3%A7as

https://www.youtube.com/watch?v=IRYbq9EMyNM
https://www.youtube.com/watch?v=TfAO8P5oVeI
https://www.youtube.com/watch?v=t43OKYEqw8U
https://zillion.com.br/seguranca-infantil-na-internet/
https://revistacrescer.globo.com/Criancas/Comportamento/noticia/2020/05/8-dicas-para-garantir-seguranca-online.html
https://blog.avast.com/pt-br/as-7-regras-de-seguranca-e-privacidade-para-criancas-na-internet


https://www.linkedin.com/in/joas-antonio-dos-santos
https://github.com/CyberSecurityUP
https://www.youtube.com/channel/UCFvueUEWRfQ9qT9UmHCw_og
THANK YOU VERY MUCH!!