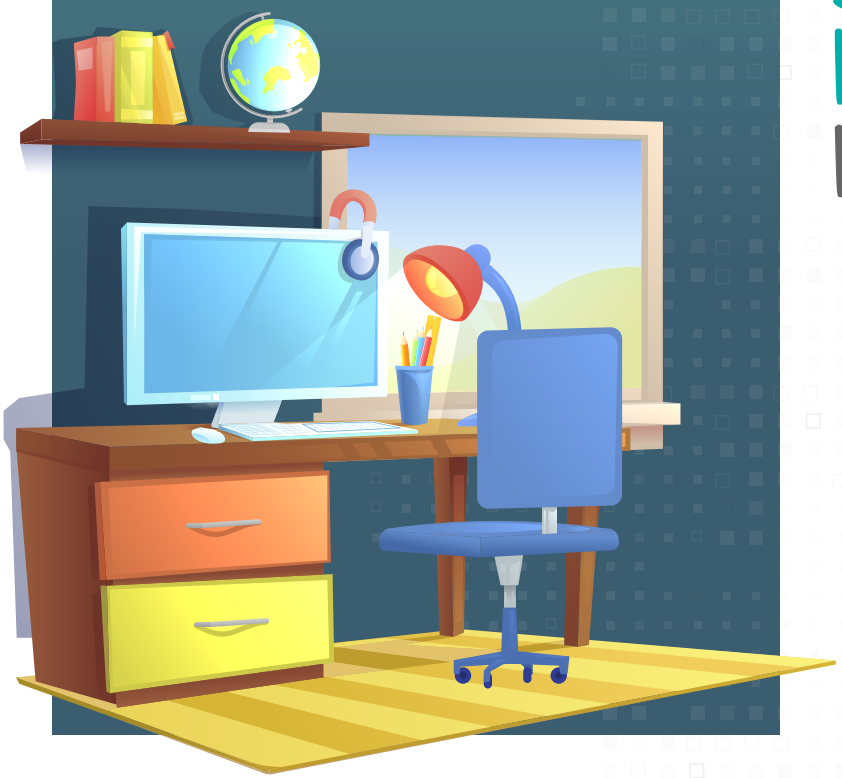
gcsecurity.com.br

WHITEPAPER

SEGURANÇA INFANTIL NA WEB



gcsecurity

GUIA DE SEGURANÇA INFANTIL NA WEB:
PORQUE ESSE GUIA FOI CRIADO?

Durante a pandemia do coronavirus (COVID-19) muitas famílias estão em quarentena nas suas casas. Com isso, além de muitos pais estarem **trabalhando remotamente**, escolas e instituições de ensino tiveram de se adaptar à **nova realidade**, disponibilizando aulas e tarefas online. As crianças estão passando muito mais **tempo online** não só por motivos acadêmicos, como também para realizar aulas extracurriculares e para socializar através de bate-papos com amigos.

Estar conectado ameniza o impacto do isolamento social dentro de casa e ajuda crianças e adolescentes a seguirem suas vidas o mais próximo da normalidade possível agora. Porém, esse "novo normal" apresenta muitos **desafios para os pais**. Como é possível maximizar tudo de bom que a internet tem a oferecer, minimizando os **potenciais danos**? Crianças e adolescentes são especialmente vulneráveis no ambiente online. Os riscos podem ter consequências severas e até trágicas. De predadores cibernéticos a postagens inadequadas em redes sociais, crianças podem involuntariamente se expor e expor suas famílias a ameaças de todos os tipos. **Proteger as crianças** na internet é questão de **conscientização** – saber quais são os perigos e como protegê-las.

Primeiro, entenda os possíveis **riscos:**

CYBERBULLYING

Hoje, as redes sociais e jogos online representam o **playground virtual**, que funciona 24 horas por dia. É aí que acontece o bullying cibernético. Crianças podem ser ridicularizadas em conversas nas redes sociais, ou em jogos online onde seus personagens podem ser submetidos a ataques incessantes, por exemplo. Existem **softwares de segurança** e aplicativos especializados para monitorar a atividade online do seu filho, mas a melhor prevenção é o **diálogo aberto**.

PREDADORES CIBERNÉTICOS

A falsa **sensação de anonimato** que a internet oferece, somada à inocência das crianças e à falta de supervisão de adultos, faz com que algumas pessoas aproveitem para se aproximar e cometer crimes, como pornografia infantil e chantagem.

INFORMAÇÕES PESSOAIS

Crianças não entendem os **limites sociais**, por esse motivo podem postar **informações pessoais**, desde imagens a localizações, que possivelmente colocam em risco tanto elas mesmas, como também suas famílias.

PHISHING

Pode ser mais difícil para as crianças de detectar **links ou anexos maliciosos**, cibercriminosos podem criar e-mails que pareçam legítimos ou inofensivos, mas que carregam ameaças e roubam dados pessoais. Uma tática muito usada é **coletar informações** em sites infantis populares ou em rede sociais para direcionar o ataque, enviando mensagens em nome de algum personagem ou ente querido, por exemplo.

GOLPES

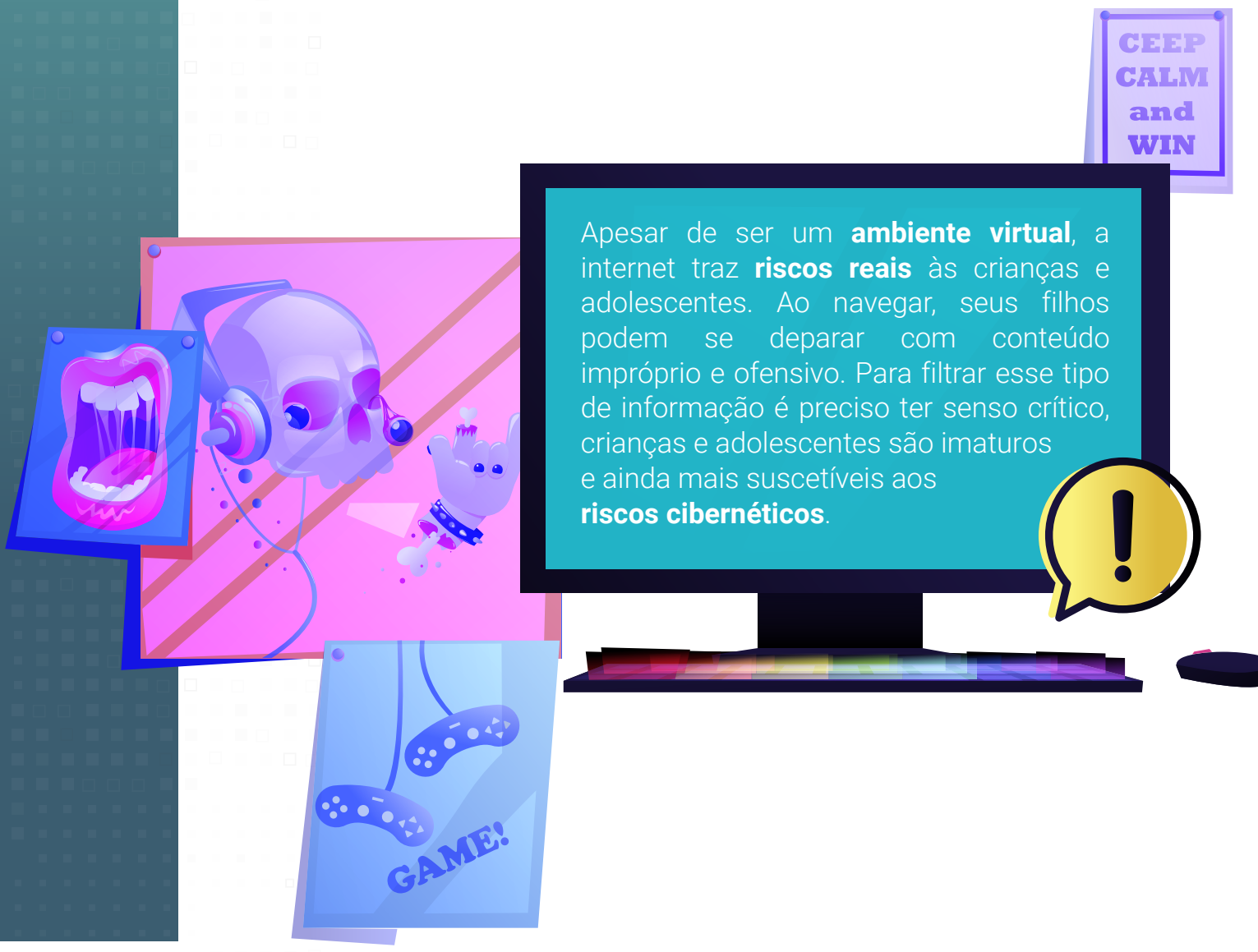
Assim como em alguns casos de phishing, criminosos pode usar **sites populares** entre crianças e adolescentes para identificar potenciais vítimas e, em seguida, prometer prêmios em **troca de informações** - como dados de cartões de crédito.

MALWARE

Trata-se de um software que é **instalado sem o conhecimento** ou permissão da vítima e realiza ações prejudiciais no computador, incluindo o registro de tudo o que é digitado no teclado, conteúdo de telas e captura de vídeos da webcam. Crianças e adolescentes podem **acidentalmente clicar** em links maliciosos e instalar essas ameaças em seus dispositivos. Jogos falsos nas lojas de aplicativo também são uma tática muito utilizada, eles solicitam permissões de acesso a contatos, câmera e sistemas do celular, podem monitorar continuamente a localização, roubar dados e facilitar outros golpes.

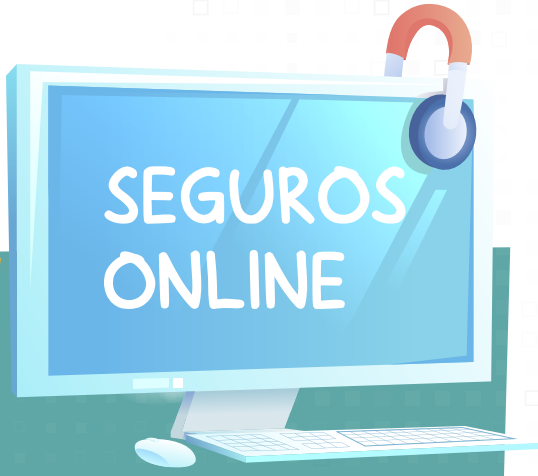
POSTS

Não existe a tecla "delete" na internet. Tudo o que acontece online, fica online e deixa rastros. É preciso **orientar crianças e adolescentes** para terem cuidado com tudo o que postam.

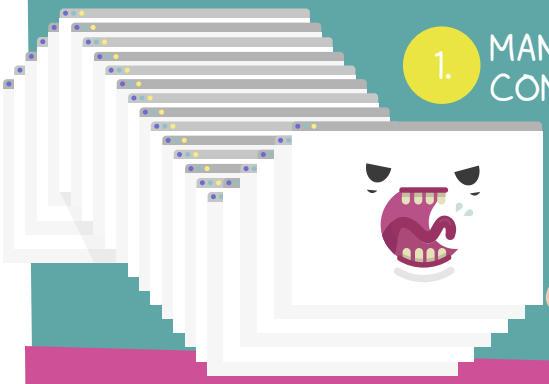


Apesar de ser um **ambiente virtual**, a internet traz **riscos reais** às crianças e adolescentes. Ao navegar, seus filhos podem se deparar com conteúdo impróprio e ofensivo. Para filtrar esse tipo de informação é preciso ter senso crítico, crianças e adolescentes são imaturos e ainda mais suscetíveis aos **riscos cibernéticos**.

O UNICEF LISTOU 5 MANEIRAS PARA AJUDAR A MANTER CRIANÇAS E ADOLESCENTES



1. MANTENHA UMA COMUNICAÇÃO ABERTA



Tenha um **diálogo honesto** com seus filhos sobre com quem eles se comunicam e como.
Fique atento às **emoções** e **atitudes**, que podem indicar algo anormal, como se seu filho está escondendo algo ou sofrendo **cyberbullying**.
Estabeleça regras de uso, incluindo como, quando e onde os dispositivos podem ser usados.

2. USE TECNOLOGIA PARA PROTEGÊ-LOS

Verifique se o dispositivo do seu filho está com **software** e **antivírus atualizados**, e que as configurações de privacidade estão em funcionamento.
Mantenha as **webcams cobertas**.
Para crianças mais novas, ferramentas como controles parentais, incluindo os de pesquisa segura, podem ajudar a manter uma experiencia online positiva.
Cuidado com os recursos educacionais online gratuitos! **Nunca se deve fornecer dados pessoais** como fotos ou nome completo para utilizar esse tipo de recurso.

3. PASSE TEMPO ONLINE COM SEUS FILHOS TAMBÉM

Aproveite a oportunidade e sirva de exemplo: conecte-se com os outros com **bondade** e **empatia** em suas **interações virtuais**, ajude-os a reconhecer e evitar conteúdos inadequados para a idade e evitar desinformação, incluindo conteúdos sobre **COVID-19**. Existem fontes excelentes com recursos digitais de organizações confiáveis disponíveis para pais e filhos aprenderem mais sobre a pandemia.
Procure com seu filho aplicativos, jogos e outras fontes de entretenimento online **adequados para a idade**.

4. INCENTIVE HÁBITOS POSITIVOS ONLINE

Esteja atento às chamadas de vídeo de seus filhos, e incentive o bom comportamento.
Passando mais tempo online, crianças estão mais sujeitas a anúncios que podem promover **estereótipos de gênero** ou **material inadequado para a idade**. Ajude-os a reconhecer esse tipo de publicidade e entender o que há de errado com algumas mensagens que podem ter efeitos negativos.

5. INCENTIVE A DIVERSÃO, ATIVIDADE E EXPRESSÃO

Algumas redes sociais, quando utilizadas com bom-senso e consciência, se tornam ótimas ferramentas para explorar a **expressão** e **criatividade** das crianças e adolescentes.
Outras ferramentas digitais promovem atividades que os fazem levantar e se mover, para escapar da **letargia** e **sedentarismo**.

https://www.unicef.org/

Confira algumas orientações básicas da Cartilha de Segurança para Internet para usar a internet de forma responsável e segura:

- **Pense bem** antes de postar algo na internet. Depois será difícil remover.
- **Não poste**, **não curta** e **nem compartilhe** conteúdos que prejudiquem outras pessoas.
- **Cuidado com estranhos** ou pessoas que você conhece apenas da internet. Não forneça dados pessoais e **nunca marque encontros**.
- **Cuidado com desafios perigosos**. Não coloque a sua saúde e nem a dos outros em risco.
- Curtidas são legais, mas **sem exageros**.
- **Use sempre um apelido** quando estiver jogando online.
- **Peça ajuda** se alguém estiver incomodando você.
- Mantenha seu **perfil privado** nas redes sociais.
- Suas **senhas são secretas**, não compartilhe!
- Faça sempre **backup** dos seus arquivos.
- Mantenha seus equipamentos **sempre atualizados**.
- Cuidado com **links maliciosos**!

gcsecurity

+55 (11) 2972-8999
contato@gcsec.com.br
São Paulo - SP
Rua Jaceru, 384, conjunto 1907
Vila Gertrudes • 04705-000
www.gcsecurity.com.br

Sobre a GC

Surgimos em 2008 e, desde então, trabalhamos incansavelmente para reduzir os riscos digitais em companhias de todos os setores e portes.

Ampliamos a visibilidade sobre vulnerabilidades e falhas de segurança para proteger ativos, dados, aplicações, usuários e sistemas.

Criamos um framework exclusivo que inclui práticas dos mais avançados padrões de segurança de mercado como NIST, PCI-DSS, ISO 27.001 e 27.005 e guiamos nossos clientes através da prevenção de riscos digitais, proteção e continuidade de negócios.

Pessoas

Nossa equipe é formada por mais de 20 profissionais especializados em segurança cibernética, com formação multidisciplinar, certificações técnicas e grande capacidade de pesquisa e desenvolvimento de proteções contra ameaças digitais.

A expertise em cyber security, gestão de vulnerabilidades, compliance, gestão de risco digital e ethical hacking permite que a gente crie soluções eficientes, sempre um passo à frente das táticas de ataque usadas por cibercriminosos.