

Preparando as famílias e suas crianças
para a segurança no mundo digital

ANZIIDS

"VOCÊ SABE TUDO QUE
POSSO FAZER COM O QUE
VOCÊ POSTA?"

HACKER

#1



Comece por aqui.

Criamos este material pensando em você, **sua família** e, principalmente, nas **crianças e adolescentes** que crescem em um mundo cada vez mais conectado.

A tecnologia oferece oportunidades incríveis de aprendizado, diversão e desenvolvimento. Ao mesmo tempo, ela traz **desafios** que exigem atenção, diálogo e orientação. Por isso, reunimos neste material dicas práticas e informações importantes para ajudar pais e responsáveis a promoverem uma **experiência digital mais segura**, saudável e consciente.

Somos uma empresa especializada em Segurança da Informação, com mais de 12 anos de experiência na proteção de pessoas e organizações no ambiente digital. Também integramos o grupo do **Movimento Desconecta de Bragança Paulista**, que nos inspirou e apoiou na criação deste projeto.

Mais do que compartilhar conhecimento técnico, queremos **contribuir** para que famílias se sintam mais preparadas para orientar, proteger e acompanhar seus filhos na construção de hábitos digitais seguros.

Esperamos que este conteúdo **fortaleça as conversas** dentro de casa e ajude a transformar a segurança digital em um tema natural do dia a dia. Afinal, cuidar da presença digital de uma criança é também cuidar de seu futuro, de sua privacidade e de seu bem-estar.

Desejamos uma excelente leitura para toda a família!



O que é exposição digital ?

ANZIKIDS



Tudo o que publicamos na internet conta uma história sobre nós e nossa família. Muitas vezes, sem perceber, compartilhamos informações que podem ser utilizadas por pessoas mal-intencionadas. Fotos, localização, rotina, escola das crianças, viagens, bens materiais e até momentos do dia a dia podem servir como peças de um quebra-cabeça digital. Quando reunidas, essas informações ajudam terceiros a conhecer hábitos, vulnerabilidades e oportunidades de exploração.

Por trás de muitos **crimes digitais** existe uma combinação simples: informação disponível, oportunidade e motivação. Um criminoso não precisa invadir sistemas sofisticados quando encontra nas redes sociais dados suficientes para aplicar golpes, praticar engenharia social ou até mesmo monitorar a rotina de uma família.

Por isso, é importante refletir antes de publicar!

Pergunte-se: ***Esta informação realmente precisa ser compartilhada?***

Quem poderá vê-la? Como ela poderia ser interpretada ou utilizada por alguém desconhecido?

A segurança digital começa com pequenas escolhas diárias. Compartilhar menos não significa viver com medo, mas sim proteger aquilo que tem mais valor: ***a privacidade, a segurança e o bem-estar da sua família.***

Phishing – Te pescando....



O phishing é um dos primeiros temas que vamos abordar nesta cartilha, porque ele está por trás de muitos golpes que acontecem todos os dias na internet.

O nome pode parecer complicado, mas a ideia é simples: alguém tenta enganar você para conseguir informações, dinheiro ou acesso às suas contas.

E esses golpes estão cada vez mais sofisticados. Com o avanço da Inteligência Artificial, mensagens falsas, perfis clonados, áudios e até vídeos podem parecer extremamente reais.

Porque invadir se posso fazer você
abrir a porta para mim?

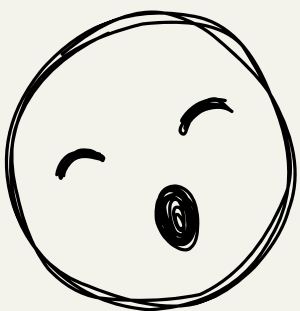
Phishing – Te pescando....

E quando isso acontece, muitas vezes a pessoa já foi "pescada" sem nem perceber.

As portas de entrada são inúmeras: redes sociais, jogos online, WhatsApp, SMS, e-mails, aplicativos de mensagens e até ligações telefônicas. Os criminosos exploram a curiosidade, a urgência, o medo e até o desejo de ajudar alguém para induzir decisões rápidas.

Como regra inicial, ensine sua família a sempre desconfiar quando:

- Alguém pedir senhas, códigos de verificação ou dados pessoais.
- Uma mensagem criar senso de urgência, como "responda agora" ou "sua conta será bloqueada".
- Um link chegar de forma inesperada, mesmo vindo de alguém conhecido.
- Houver promessas boas demais para serem verdade.
- Uma criança for incentivada a manter segredo sobre uma conversa online.



A melhor defesa não é a tecnologia, mas o hábito de parar por alguns segundos e verificar antes de clicar, responder ou compartilhar informações.



Mas afinal, o que
motiva um hacker?

VINGANÇA



**Alguns ataques são motivados
por conflitos pessoais,
ressentimentos ou desejo de
prejudicar alguém.**

Possíveis ataques:

Exposição de informações privadas.
Vazamento de fotos, mensagens ou
documentos.

Invasão de redes sociais e e-mails.
Publicações falsas utilizando a identidade
da vítima.

Tentativas de prejudicar a reputação da
pessoa ou da família.

DINHEIRO



**Esta é a motivação mais comum.
Criminosos digitais procuram transformar
informações em lucro.**

Possíveis ataques:

Roubo de senhas bancárias.

Golpes via PIX.

Clonagem de contas de WhatsApp.

Extorsão e sequestro de dados.

Venda de informações pessoais na internet.

FAMA



Alguns invasores buscam reconhecimento
dentro de grupos e comunidades online.
Para eles, demonstrar que conseguiram
invadir uma conta ou sistema funciona
como uma forma de ganhar status.



Deflagrada operação que visa reprimir ação de criminosos que se passavam por policiais federais

Investigação apura a utilização de identificação falsa de policiais federais para extorsão de vítimas que recebiam imagens de meninas nuas

 Atmosfera On.line / Aug 11, 2021

Golpes utilizando perfis falsos

Nem os criminosos estão seguros dos perigos da internet. Um desdobramento da operação Dólos foi que outros criminosos aproveitaram-se das situação e criaram perfis falsos de crianças justamente para atrair pedófilos para posteriormente se passarem por agentes da Polícia Federal exigindo o pagamento de uma propina para que não sejam investigados. Mais uma vez, atraindo o alvo e explorando suas vulnerabilidades. (Embora seja irônico)

"Nem toda pessoa online é quem diz ser."



Brazil Hit by Banking Trojan Spread via WhatsApp Worm and RelayNFC NFC Relay Fraud

Water Saci and RelayNFC drive advanced Brazil-targeted attacks using WhatsApp worm tactics and real-time NFC payment theft.

 The Hacker News

Malware espalhado por mensagens de contatos conhecidos.

Notícia que repercutiu até mesmo no exterior. Nesse ataque, um dispositivo é infectado e passa a enviar mensagens pelo WhatsApp da vítima para seus contatos, solicitando a abertura de um documento malicioso. Esse documento instala o malware no novo dispositivo, permitindo o roubo de dados e sua propagação para outras vítimas. Trata-se de um exemplo clássico de ameaça que explora a confiança entre pessoas para se espalhar.

"Confiar na pessoa que enviou a mensagem não significa que o conteúdo seja seguro."



3 hábitos para começar hoje

Converse regularmente com seus filhos.

- Pergunte o que eles fazem online.
- Conheça os jogos, aplicativos e redes sociais que utilizam.
- Crie um ambiente onde eles se sintam seguros para pedir ajuda.

Compartilhe com consciência.

- Evite divulgar rotina, localização e informações pessoais.
- Pense antes de postar fotos das crianças.
- Lembre-se: cada publicação revela um pouco sobre sua família.

Pare. Pense. Verifique.

Antes de clicar, responder ou compartilhar:

- Quem enviou?
- Eu estava esperando essa mensagem?
- Esse pedido faz sentido?
- Existe alguma pressão para agir rapidamente?



Se liga!

O que levar deste material?

A maioria dos golpes não começa com uma invasão.

Ela começa com:

- Uma conversa.
- Um clique.
- Uma mensagem.
- Uma publicação compartilhada sem pensar.

O que os criminosos procuram?

- Informações sobre sua rotina.
- Dados pessoais e financeiros.
- Fotos e informações da família.
- Crianças e adolescentes vulneráveis a abordagens online.
- Oportunidades para explorar confiança, curiosidade e distração.



Lembre-se

- Nem toda pessoa na internet é quem diz ser.
- Nem toda mensagem merece confiança.
- Nem todo link deve ser aberto.
- Nem toda informação precisa ser compartilhada.

A segurança
digital começa
em casa.



A tecnologia continuará evoluindo.
Novos aplicativos surgirão.
Novos golpes também.

Mas crianças que aprendem a:

- Pensar antes de clicar;
- Questionar antes de acreditar;

Conversar antes de agir;

**Estarão muito mais preparadas para
navegar com segurança no mundo
digital.**

A segurança digital não é uma conversa única.
É um hábito construído todos os dias, em família.



Quer saber mais?

Inscreva-se em nossa newsletter e receba as próximas edições.

