



Digipais

UMA INICIATIVA DA **saferkidsonline** by **eset**



**O roubo de identidade
também afeta as crianças**

De vez em quando, nossa equipe de cibersegurança da ESET recebe consultas sobre casos em que a identidade de um menor foi roubada na Internet, e seus familiares e amigos estão em busca de ajuda para saber como proceder.

O que a um simples olhar poderia parecer um incidente breve e desagradável, na maioria dos países é considerado um delito, e, por isso, os pais ou tutores legais das vítimas jovens de roubo de identidade **devem entrar em contato com a polícia local ou buscar assessoramento legal**. Recomendamos que o façam, já que, longe de ser um incidente menor, **o roubo de identidade pode ter um impacto grave no futuro financeiro dos seus filhos**.

O roubo de identidade afeta até crianças muito pequenas

O roubo de dados pessoais on-line é muito comum. Talvez você pense que os dados dos seus filhos não tenham muita utilidade. Mas, quando forem maiores, **terão um histórico de crédito limpo sem antecedentes penais, algo que os golpistas podem aproveitar em benefício próprio**.

Ainda que se prove legalmente que quem fez um empréstimo ou recebeu uma multa foi um terceiro que usou indevidamente seu nome, seus filhos terão problemas administrativos que custará muita burocracia para resolver.

Cuidado com a engenharia social

Os ladrões de identidade geralmente tentam roubar os nomes, os endereços, os números de passaporte ou identificação e, em certos casos, os dados financeiros de vítimas anônimas. Alguns compram esses dados na Dark Web (sites que não podem ser encontrados no Google) e outros usam malware ou táticas de engenharia social para obtê-los por seus próprios meios.

Assim que conseguem infectar os dispositivos das vítimas com malware, os cibercriminosos podem extrair os dados pessoais armazenados nos dispositivos ou navegadores de Internet. Se usarem um malware para registrar as pulsações, tudo o que a vítima escreve em seu dispositivo infectado é enviado diretamente ao atacante, incluindo números de cartões de crédito e senhas.

Também há outra forma de ataque mais rentável para os golpistas on-line: a engenharia social, que consiste simplesmente em **enganar as vítimas para que elas mesmas forneçam seus dados pessoais, seja fazendo se passar por outra pessoa ou construindo um website falso**.

Isso é perigoso para as crianças que muitas vezes não têm as ferramentas para diferenciar estas situações. Mas, se você seguir esses passos simples, você irá fortalecer a proteção dos dados pessoais dos seus filhos.



Como proteger sua família do roubo de identidade

1 **Ensine a seus filhos a não compartilhar dados desnecessariamente**

Converse com eles sobre como usam as redes sociais e o que gostam de publicar, em geral. Explique porque não devem inserir o endereço de sua casa ao aceitar solicitações de amizade de pessoas que não conhecem.

2 **É imprescindível criar bons hábitos de uso de senhas**

Ensine a sua família como criar senhas longas, difíceis de adivinhar e únicas, ou a usar um administrador de senhas. Lembre-se de que não devem reutilizar senhas para diferentes serviços ou websites.

3 **Proteja a todos os dispositivos da sua família**

E apenas envie dados pessoais on-line quando sua conexão a internet for segura. Isso significa que você deve evitar usar as redes de Wi-Fi públicas ou

qualquer conexão com a internet que não seja de confiança. Em uma conexão não segura, os golpistas podem interceptar facilmente todos os formulários que você envia.

4 **Desfaça-se dos documentos confidenciais de forma segura**

Se você necessita se desfazer de documentos físicos velhos que contenham dados pessoais, destrua-os.

Não esqueça que os dispositivos eletrônicos e de armazenamento de dados que já não usa também contêm muita informação pessoal. Alguns desses dispositivos oferecem uma função para apagar dados, para se desfazer de maneira segura de todos os dados guardados.

5 **Ensine a seus filhos a identificar mensagens suspeitas**

Ou websites que poderiam tentar enganá-los para que enviem seus dados pessoais. Considere usar um Anti-Phishing, que pode ser incluído como par-



te de uma solução de segurança cibernética. Desta forma, se algum membro da família tentar abrir um website de phishing, a solução antimalware irá advertir isso a você.

Próximos passos

Mas o que você deve fazer se descobrir que os dados pessoais de seus filhos já foram roubados e foram usados para uma atividade ilícita? Não hesite: contate a polícia local. De uma forma ou outra, na maioria dos países e regiões, o roubo de identidade é considerado um crime.

Quando entrar em contato com a polícia, **leve em consideração que é possível que não estejam familiarizados com todos os aspectos deste campo da lei.** Se acontecer isso, não hesite em voltar a se apresentar com um advogado.

Ainda que não aconteça sempre, em alguns casos existe uma forte conexão entre a fraude e o bullying. Isso significa que, em alguns casos, pode ser que o atacante conheça seu filho pessoalmente. Neste sentido, é importante entrar em contato com a escola e com a família para saber se é necessário proceder de alguma outra forma.

O roubo de identidade é subestimado por muitas pessoas, por isso, se você suspeita que sua família foi vítima de um desses casos, recomendamos que se consulte com as organizações do seu país que oferecem assessoramento legal geral ou específico em segurança informática.



