Estas são as formas mais comuns de alguém te espionar na web; previna-se!...

Entrar em um computador doméstico é bem mais simples do que se imagina, e não requer habilidades ultra especiais. Então, fique esperto e veja como evitar que a sua privacidade seja invadida.

O jeito mais fácil de acessar um dispositivo é fazendo com que você baixe sem perceber um software espião, que dá acesso a dados preciosos e permite um monitoramento profundo da sua vida.

País	Prejuízo (US$ Bilhões)
China	66,3
Brasil	22

Esse tipo de golpe é chamado phishing. Ele usa emails, links no WhatsApp ou sites falsos (com cara de verdadeiros) para te fazer clicar em endereços enganosos, que escondem um software malicioso que se instala no computador ou celular. Outra coisa que acontece é que, ao digitar a senha e o login de um site que você acha que é verdadeiro, acaba fornecendo sem perceber essas informações aos criminosos.

> *"O spyware é um malware (vírus) que se usa para espionar por meio da câmera ou do microfone do dispositivo e obter acesso a informações pessoais, dados bancários, atividades online...*
>
> ***Luis Corrons***, especialista em segurança da Avast

Acesso a webcam

Isso mesmo que você leu. Esses programas, que são facilmente encontrados na internet, dão acesso à sua webcam. Com eles, é possível transformar o computador afetado em uma câmera de vídeo. É possível ver e ouvir tudo o que você faz em casa ou

no ambiente de trabalho. É por isso que sempre falamos para você cobrir a webcam com uma fita.

Como resolver: sempre digite o endereço de uma página direto na barra do navegador (ou seja, não clique em links que podem ser falsos) e observe. Se aparecer https://, quer dizer que o site usa um protocolo de segurança verificado. Não

clique naquelas correntes que recebe no WhatsApp, não abra qualquer promoção que recebe no email e nunca dê informações pessoais a sites que você não tem certeza que são confiáveis. E mais uma vez: cubra sua webcam. Normalmente, a luz ao lado da sua câmera indica se ela foi ativada ou não, mas existem ferramentas para impedir que esse alerta seja acionado.

De olho no que você digita

Outro meio de espionagem são os softwares keyloggers, que registram quais teclas são pressionadas em um teclado. Com eles, dá para saber o conteúdo das mensagens e emails que você enviou e também coletar senhas e logins. Normalmente, o seu computador passa a hospedar um keylogger quando você baixa sem perceber um software que veio escondido entre arquivos enviados por alguém. Mas existem versões físicas, que são instaladas nas portas de entrada do computador.

> *"Usam a engenharia social para tirar vantagem do comportamento humano, pois é mais fácil enganar uma pessoa do que invadir um sistema*
>
> ***Corrons***

"PODE ENTRAR"

No computador ou notebook, é possível usar ferramentas de execução remota, como o Psexec, da Microsoft, para espionar um alvo. Esse tipo de software serve para ações totalmente legais --um exemplo comum é a empresa usar esse programa para acessar remotamente o computador de um funcionários. O problema é quando isso é feito sem a pessoa saber. Instalado em um celular, um programa spyware pode rastrear a sua localização, ler mensagens de texto e redirecionar chamadas para outro aparelho, por exemplo.

Normalmente, esse tipo de programa malicioso acessa seu dispositivo quando você clica em links ou abaixa arquivos, mas pode acontecer de ser instalado pessoalmente por outra pessoa, então cuidado com quem tem acesso aos seus aparelhos.

Como resolver: além de passar um antivírus, mantenha tanto o software quanto o sistema operacional sempre atualizados --a cada nova versão, as empresas tentam corrigir falhas e pontos de vulnerabilidade da ferramenta. E não esqueça de proteger bem celulares e computadores, com senhas fortes.

Dicas para criar uma senha segura

1. Use um gerenciador de senhas
2. Use no mínimo 8 caracteres
3. Troque letras por números semelhantes (E por 3, por exemplo – m4r14 (maria))
4. Associe com algo conhecido (... você é luz, é raio estrela e luar... pode virar VoLuRaEsLu
5. Adicione símbolos (#$@&*)
6. Troque a sequencia das letras (Por Ex. Martim pode virar timMar)

Fonte: https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/03/11/hackers-podem-te-espionar-pela-camera-mas-nao-so-saiba-como-se-prevenir.htm