Dicas para se proteger de Cyberstalkers

O que é cyberstalking?

A definição de cyberstalking é muito simples, “o uso da internet, ou outros meios eletrônicos, para assediar e intimidar uma vítima selecionada”.

As características comuns incluem (mas não estão limitadas a) comportamento clássico de 'perseguição' — rastrear a localização de alguém e monitorar suas atividades online e no mundo real. Sabe-se que os cyberstalkers instalam dispositivos GPS nos carros de suas vítimas, usam spyware de geolocalização em seus telefones e rastreiam obsessivamente o paradeiro de suas vítimas por meio da mídia social.

Cyberstalking pode incluir outro comportamento destinado a intimidar as vítimas ou tornar suas vidas insuportáveis. Por exemplo, os ciberperseguidores podem ter como alvo suas vítimas nas mídias sociais, trollando e enviando mensagens ameaçadoras; eles podem hackear e-mails, para se comunicar com os contatos da vítima, incluindo amigos e até empregadores. A perseguição nas redes sociais pode incluir a falsificação de fotos ou o envio de mensagens privadas ameaçadoras. Freqüentemente, os ciberperseguidores espalham rumores maliciosos e fazem acusações falsas, ou até mesmo criam e publicam pornografia de vingança. Eles também podem se envolver em roubo de identidade e criar perfis falsos de mídia social ou blogs sobre a vítima.

cento das vítimas são na verdade homens.

Cyberstalking vai muito além de apenas seguir alguém em uma rede social. É a intenção de intimidar, que é a característica definidora do cyberstalking.

Your privacy is important
Shield yourself with webcam security, included in our premium product.
Kaspersky Total Security
Explore Now

Como evitar ser perseguido online

Um bom exercício que você deve realizar agora é pesquisar no Google e descobrir exatamente quais informações um potencial cyberstalker pode encontrar online. Você pode ficar chocado com a facilidade de localizá-lo. Sem mencionar, encontre seu endereço residencial, número de telefone e outros detalhes pessoais.

E se isso for ruim, você pode verificar quantos dados alguém poderia compilar sobre você se também tivesse acesso às mídias sociais de seus amigos e familiares. Por exemplo, eles podem descobrir em qual bar você estava, com quais amigos, ou onde você sairá de férias e quando.

You might even find stuff purporting to be from you that someone else has uploaded: a fake blog, or a Craigslist account putting your phone number and home address out there.

This is how cyberstalkers get started - Googling their victims and finding out everything they can. That means you'll certainly want to make that information as hard to obtain as possible.

Tips for protecting yourself from cyberstalkers

Increase your privacy settings

Start off with your own data. Take a good look at your social media accounts and if you haven't done already, enable strong privacy settings.

- Make your posts 'friends only' so that only people you know get to see them.
- Don't let social networks post your address or phone number publicly. (You might even want to have a separate email address for social media)
- If you need to share your phone number or other private information with a friend, do so in a private message - not in a public post.
- Use a gender-neutral screen name or pseudonym for your social media accounts — not your real name
- Leave optional fields in social media profiles, like your date of birth, blank.
- Only accept friend requests from people you have actually met in person. Set your social networks to accept friend requests only from friends of friends.
- Disable geolocation settings. You may want to also disable GPS on your phone.

If other personal data is up on the web outside your social media accounts, start removing it. In the case of your SSN being displayed, Google will help you remove that. You may need to contact third party websites to get some of the data taken down. If you

If you are using an online dating service, don't provide your full ID on the site or over email. Only give out your phone number to someone you've actually met and wouldn't mind seeing again. The best security advice is to not even give your full name online, only your first.

Be cautious of any incoming phone calls or emails which ask you to give personal information, however reasonable the purported request. If a bank or credit card company phones, get off the phone, and use another phone (for instance, if they rang your landline, use your cellphone) to ring back to verify, using the HQ or branch phone number that's on your paperwork — not the one you've just been given. And never, never, never give out your SSN.

Secure your PC and phone

Securing your data won't help you if your smartphone or PC is hacked. To prevent being stalked online you should build basic security into your online life.

- Be wary of public Wi-Fi, which can be hacked easily. If you need to log on in Starbucks or hotels, ideally use a Virtual Private Network (VPN) to prevent anyone from eavesdropping on your communications. Kaspersky's VPN can give you a secure connection wherever you are.

- Be careful where you leave your smartphone. It's not difficult to install spyware without leaving a trace - just leaving your phone on your desk for a few minutes is long enough.
- Make sure your phone and computers are password protected. Use a strong password, not something easy to guess, and reset your passwords regularly.
- Use anti-spyware software to detect any malicious software that's installed. Delete it, or better still, back up your data, then do a factory reset to ensure the spyware is completely eradicated. Kaspersky's antivirus comes in both PC and Android versions to keep all your devices safe.
- Remember to always log out of your accounts when you're done — don't leave social network accounts running.
- Beware of installing apps that want access to your Facebook or other contact lists. Do you know what they're planning to do with it?

What is catfishing?

Catfishing is a form of fraud or abuse where someone creates a fake online identity to target a particular victim. Catfishers may lure their victims into providing intimate photos or videos, then blackmail them, or may develop a relationship and then ask for money for a sudden emergency.

Catfishers can be very convincing, but you can discover their scam in several ways.

- If all their online photos are selfies or studio shots, with no other friends, no family, and no context, that's a big clue.
- Do a Google reverse image search against the online photo on a dating site. You may find the person has multiple online profiles with the same photo but different names.
- Ask if you can do a video call on Skype. Guess what? Catfishers will usually make their excuses - and you won't hear from them again.

What to do if you're cyberstalked

If you're being stalked online don't wait and hope the problem will go away — act immediately.

- Make it clear to the cyberstalker that you don't want to be contacted. Put it in writing, and warn them that if they continue, you'll go to the police. Don't engage with them at all once you have issued this warning.
- And if they continue, go to the police. Many police departments have a special cyberstalking team, but they're not going to quibble about a cyberstalking definition.

- If you think someone is tracking you through spyware, don't use your own computer or phone to get help - borrow a family or friend's phone.
- Get your computer and phone checked over by a professional for spyware or other signs of compromised accounts.
- Change all your passwords.
- In the case of social media stalking, use your privacy settings to block the person, and then report the abuse to the network. You can easily find out how to report cyberstalking in most social networks' help and support pages.
- If you have been sent abusive or threatening emails, you probably know the stalker's ISP - the bit after the @ in their email address. Contact abuse@domainname or postmaster@domainname. Most ISPs take cyberstalking very seriously. If they're using Gmail, there's a reporting mechanism you can use at https://support.google.com/mail/contact/abuse.
- You can filter abusive emails to a separate folder so that you don't have to read them.
- If you think the cyberstalker might harass you in the workplace, tell your employer.

Save copies of any communications involved, including your own, police reports, and emails from the networks. Back up the evidence on a USB stick or external drive.

Cyberstalking laws

O cyberstalking está sujeito a leis gerais sobre assédio, como o Violence Against Women Act de 1994 nos EUA e o Protection from Harassment Act de 1997 no Reino Unido. A Califórnia criou a primeira lei estadual abordando especificamente o cyberstalking como uma ofensa em 1999, e outros estados seguiram o exemplo.

É bom que o cyberstalking agora seja reconhecido como o crime sério que é: o cyberstalking pode destruir a vida das pessoas, mas não precisa destruir a sua.

Links Relacionados

Anatomia de golpes de namoro online - como não se tornar uma vítima de ciber-romance

O que fazer se sua conta de e-mail for invadida

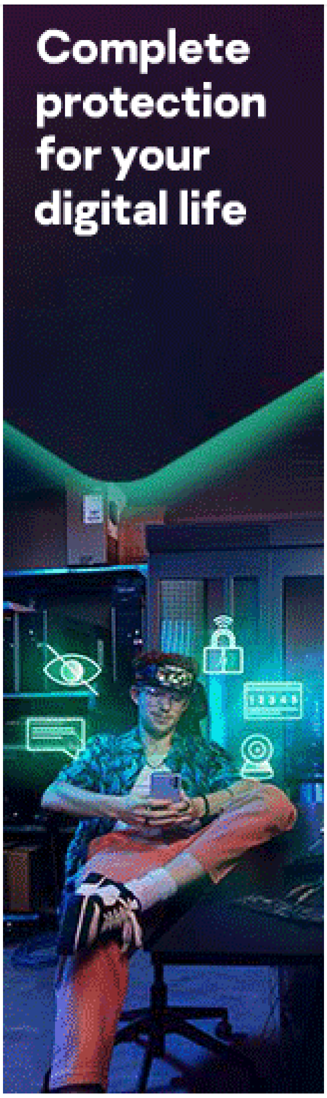
O que é spyware? - Definição

Quão seguras são as carteiras eletrônicas? Como proteger sua carteira eletrônica

Não seja uma vítima de phishing: o convite do seu evento online é seguro para abrir?

Fui vítima de ataques de phishing! E agora?

Os 10 maiores riscos de jogos online e como evitá-los



Protegendo você, sua família e muito mais

Obtenha o poder de proteger. Descubra como nossa segurança premiada ajuda a proteger o que é mais importante para você.

Obtenha ferramentas GRATUITAS

Há uma ampla gama de ferramentas GRATUITAS da Kaspersky que podem ajudá-lo a se manter seguro – em dispositivos PC, Mac, iPhone, iPad e Android.

Nós estamos aqui para ajudar

Ajudar você a ficar seguro é o nosso objetivo – portanto, se precisar entrar em contato conosco, obtenha respostas para algumas perguntas frequentes ou acesse nossa equipe de suporte técnico.

Quem nós somos

Descubra por que estamos tão comprometidos em ajudar as pessoas a se manterem seguras... online e além.

Obtenha sua avaliação gratuita

Desconto para estudantes

Students save on the leading antivirus and Internet Security software with this special offer.

Stay in Touch

Home Solutions

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

All Solutions

Small Business Products
(1-50 EMPLOYEES)

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products
(51-999 EMPLOYEES)

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions
(1000+ EMPLOYEES)

Cybersecurity Services

Threat Management and Defense

Endpoint Security

Hybrid Cloud Security

All Products

United States

Contact Us • About Us • Partners • Blog
• Resource Center • Press Releases • Sitemap • Careers