AUTORIA

Amarelu e Martu Isla (Amartu)

AGRADECIMENTOS

Muito obrigade à companheires de Navegando Libres, Fembloc, Luchadoras e Maria d'Ajuda por seu tempo e por compartilharem tantas ideias. Esperamos que este material retribua e esteja à altura de seu extraordinário trabalho.

Muito obrigade à Rede Transfeminista de Cuidados Digitais, por compartilhar sua infraestrutura digital.

Muito obrigade também a Ariel, Lux, Foz, Tes, Inés e todes que dedicaram tempo para revisar o conteúdo e nos dar seu feedback.

Muito obrigade ao Center for Digital Resilience por confiar em nós para desenvolver este projeto.

VERSÃO WEB E DOWNLOADS

pt.celularhackeado.net (en Portugués)

es.celularhackeado.net (en Español)

CONTATO

amartu-zine@riseup.net

<SUE COMPANHEIRE NÃO É HACKER>

Parte 1: Desmistificando o hackeamento de celulares

Licença

@ Amartu (Amarelu e Martu) 2025

Este fanzine é licenciado com a Licença Feminista de Produção entre Pares - F2F.[34]. Com esta licença **você é livre para compartilhar a obra** (copiar, distribuir, executar ou comunicar publicamente) e para **fazer obras derivadas** sob as seguintes condições:

Atribuição: você deve **reconhecer os créditos da obra da maneira especificada pela(s) pessoa(s) autora(s) ou licenciantes** (mas não de uma maneira que sugira que apoiam o uso que você faz da obra).

Compartilhar sob a mesma licença: se você modificar ou transformar esta obra, ou produzir uma obra derivada, **você só poderá distribuir a obra gerada sob uma licença idêntica a esta**.

Feminista anticapitalista: a exploração comercial desta obra só é permitida a cooperativas, organizações, coletivos e redes sem fins lucrativos, e a organizações de pessoas trabalhadoras autogestionadas, **que se identifiquem e se organizem sob princípios feministas**. Todo excedente ou mais-valia obtidos pelo exercício dos direitos concedidos por esta licença sobre a obra não podem ser acumulados ou usados para especulação e devem ser reinvestidos na luta contra o cisheteropatriarcado e o capitalismo.

34 https://labekka.red/licencia-f2f/

- Não instale apps de fontes desconhecidas ou sem conferir bem se são realmente o que dizem ser.
- Não acredite em tudo que vê na internet. Confie apenas em sites oficiais ou fontes confiáveis.
- Reduza o número de apps no seu dispositivo.
- Experimente restaurar o celular para os valores de fábrica pelo menos uma vez por ano.

Sabemos que todos esses passos podem ser muito, então busque um lugar seguro, confortável, tempo, paciência e pessoas de confiança que possam te acompanhar.

Hackeie o patriarcado: fortaleça seus conhecimentos em tecnologia! Temos certeza que você sabe muito mais do que imagina!

Hoje em dia, os celulares são quase uma extensão do nosso corpo, dos nossos braços: **vamos dedicar o tempo necessário para entendê-los, configurá-los e fazer com que funcionem a nosso favor!**

Mas lembre-se de também de tirar momentos de descanso da tecnologia :)

Conteúdos

Introdução

Ao colaborar com linhas de ajuda feministas de cuidados digitais, percebemos que muitos mitos cercam o tema da invasão de celulares, gerando concepções equivocadas que alimentam sentimentos de impotência, angústia e paranoia entre pessoas em situação de violência. Com base nessa experiência, desenvolvemos um conteúdo para desmistificar essas ideias e oferecer informações acessíveis sobre hackeamento e análise de celulares, buscando um equilíbrio entre a gravidade dos riscos e uma abordagem cuidadosa e realista. Esperamos que este material seja útil tanto para quem enfrenta violência digital quanto para suas redes de apoio e para as próprias linhas de ajuda, que constantemente enfrentam e desconstroem esses mitos.

Para produzir este conteúdo, realizamos entrevistas com 4 linhas de apoio feministas em cuidados digitais: **Navegando Libres**, do Equador; **Luchadoras**, do México; **Maria d'Ajuda**, do Brasil; e **Fembloc**, da Catalunha. Nesses encontros conversamos sobre os mitos que cada linha identificava, os motivos pelos quais os mitos existiam, que imaginários estão por trás dessas ideias e que

5. **Revise os apps instalados**, confirme se você sabe para que serve cada um, pesquise na internet o nome do app se tiver dúvidas.

6. **Revise seu celullar com um antivírus**, você pode usar o Malwarebytes[32] (você pode usar a versão de teste e depois desinstalar) ou o Koodous[33]. Atenção: evite outros antivírus e desinstale-os após a verificação. Lembre-se: o melhor antivírus é você.

7. **Verifique se você não tem** ativadas funcionalidades ou apps de **controle parental**.

8. **Verifique a configuração de "Buscar meus dispositivos"**.

9. Use a tecnologia de forma **mais consciente e cuidadosa possível**:

- Evite o caos, use métodos ou ferramentas que te ajudem a se organizar, como um gerenciador de senhas.
- Não clique em "ok" ou "próximo" sem ler.

32 https://www.malwarebytes.com/es/
33 https://koodous.com/product/koodous-mobile

- Escolha um gerenciador de senhas com o qual você se sinta confortável (alguns recomendados são Bitwarden[28], KeePassXC[29], KeePassDX[30], 1Password[31]).
- Coloque uma senha diferente e forte para cada conta.
- Organize as senhas no seu novo gerenciador.
- Não salve suas senhas no navegador ou nos gerenciadores do Google ou Apple.
- Ative a autenticação em dois fatores para todas as contas que você considerar mais importantes.

4. **Revise suas configurações**:

- Reduza seus métodos de recuperação de conta a emails ou números de telefone que você acesse com frequência. É por esses canais que chegarão os alertas em caso de tentativa de recuperação de conta.
- Verifique as sessões iniciadas. Encerre todas as sessões que você não reconhecer.

28 https://bitwarden.com/
29 https://keepassxc.org/
30 https://play.google.com/store/apps/details?id=com.kunzisoft.keepass.free&hl=pt
31 https://1password.com/

conteúdos poderiam ser úteis para ajudar a desconstruir esses mitos.

Finalmente, decidimos organizar o conteúdo em **dois volumes distintos**, **um dedicado a desmistificar o hackeamento de celulares**, e **outro dedicado a desmistificar a análise de celulares**, que é a análise feita para detectar sinais de hackeamento.

O volume que você tem em mãos é o volume 1, onde tentamos esclarecer alguns conceitos, explicar as formas mais comuns de espionagem no celular, como softwares espiões realmente funcionam, quais sintomas podem ser preocupantes e quais não são... entre outros conteúdos que julgamos relevantes para desmistificar mitos sobre hackeamento de celulares e supostos hackers. Também adicionamos referências de onde procurar ajuda e recomendações básicas para que você mesmo possa ser hacker!

Este fanzine nasceu como o projeto final da Fellowship do Center for Digital Resilience do qual fizemos parte entre agosto de 2024 e julho de 2025. Foi um trabalho feito a quatro mãos, com quatro horas de diferença

de fuso horário, de duas margens muito distantes do Oceano Atlântico, entre o Rio de Janeiro e as Ilhas Canárias.

Neste material utilizamos linguagem neutra e o "e" para nos referirmos a qualquer pessoa que possa estar enfrentando uma situação de violência mediada pela tecnologia. Esta é uma abordagem feminista inclusiva para pessoas trans e não binárias. Esperamos que você se sinta confortável ao ler.

Esperamos que você goste e seja útil ♥

Amarelu e Martu

10. Dicas rápidas para que a pessoa hacker seja você

Sabemos que você pode estar em uma situação muito estressante, angustiante e precisando de soluções.

No entanto, queremos te avisar que, como quase tudo na vida: **não existem soluções mágicas!**

Nossas melhores dicas são:

1. **Busque apoio emocional**, esteja com suas amizades e pessoas queridas.
2. **Tente organizar sua vida digital**:

- Liste suas contas do Google, Apple ou Microsoft.
- Liste outras contas de email (Yahoo, Hotmail, etc).
- Liste suas redes sociais.
- Liste seus dispositivos (celulares, tablets, relógios, TV, computadores, etc).
- Identifique qual conta está configurada em cada dispositivo.
- Identifique os emails, números de telefone ou outros métodos de recuperação das contas de redes sociais e email.

3. **Organize e fortaleça suas senhas**:

Se você precisa de atendimento em outros idiomas e territórios, pode consultar o índice de linhas de ajuda feminista: *feministhelplines.org*.

Além disso, se você é **ativista, defensore de direitos humanos, jornalista, advogade** e/ou trabalha com temas sensíveis pelos quais governos ou outras entidades possam te perseguir, recomendamos estas linhas de atendimento:

- Access Now[23], com suporte internacional: atendimento em 9 idiomas.
- SMEX[24], do Líbano: atendimento em inglês e árabe.
- Amnesty Tech[25], com suporte internacional.
- Front Line Def[26]enders, com suporte internacional: atendimento em diversos idiomas.

A Anistia Internacional também oferece um base de dados[27] onde você pode encontrar mais organizações que podem te ajudá, em outros idiomas e contextos.

23 https://www.accessnow.org/help-pt/
24 https://smex.org/helpdesk/
25 https://securitylab.amnesty.org/es/get-help-digital-forensic-support/
26 https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders
27 https://securitylab.amnesty.org/digital-resources/

1. Fui Hackeade?

De repente seu celular começa a agir de forma estranha. A bateria descarrega rápido demais, aplicativos travam sem explicação. Você sente que tem algo errado, como se, magicamente, alguém estivesse lendo seus pensamentos ou te acompanhando à distância. Sue ex-companheire posta algo parecido ao que você acabou de comentar com uma amiga. Um print que você não lembra de ter feito surge na galeria. E, como se não bastasse, aparece para você uma sugestão de contato que é específica demais para ser só coincidência. São pequenas coisas, desconexas, mas que somadas fazem você se perguntar: "**fui hackeade?**"

Você não está alucinando, essas coisas podem realmente acontecer. Mas é importante ter cautela: nem sempre significam que você foi hackeade. Às vezes são falhas técnicas, bugs do sistema, efeitos de atualizações ou do funcionamento invasivo de algoritmos. Seja como for, isso não diminui a seriedade daquilo que você sente. **A angústia é real. A dúvida é legítima**.

E essa dúvida não surge do nada. Vivemos em um contexto de vigilância constante, e isso, por si só, já pode causar desconforto. Quando há um histórico de violência, ameaça ou conflito, seja em casa, no trabalho ou num relacionamento, é comum que o corpo entre em estado de alerta. A gente passa a prestar atenção em qualquer comportamento estranho do celular, e problemas corriqueiros podem ativar memórias, medos e mecanismos de defesa.

A falta de conhecimento sobre como funcionam os sistemas também pode contribuir para essa situação. Nem sempre sabemos o que os aplicativos realmente acessam, ou por que certas coisas aparecem na tela. Isso faz com que os celulares se transformem numa fonte constante de insegurança. **Quando a tecnologia parece incompreensível e misteriosa, ela também se torna ameaçadora**.

Além disso, esse desconhecimento também faz com que, em um relacionamento, as pessoas transfiram a tarefa de configurar o celular, instalar aplicativos, criar senhas e resolver problemas técnicos para a outra pessoa que "entende mais" de tecnologia (geralmente um ho-

para os padrões de fábrica e não deixe sua conta Google ou Apple logada.

9. Onde buscar ajuda transfeminista

Estas são algumas linhas de ajuda feminista que recomendamos:

- → Maria d'Ajuda[18], do Brasil: atendimento em português e espanhol.
- → Navegando Libres[19], do Equador: atendimento em espanhol.
- → Luchadoras[20], do México: atendimento em espanhol.
- → Fembloc[21], da Catalunha (Espanha): atendimento em espanhol e catalão.
- → Centro S.O.S. Digital de Internet Bolivia[22], da Bolívia: atendimento em espanhol.

18 https://mariadajuda.org/
19 https://navegandolibres.org/linea-de-acompanamiento-feminista/
20 https://luchadoras.mx/formulario/
21 https://fembloc.cat/
22 https://sosdigital.internetbolivia.org/

Ao entregar seu celular a uma pessoa, você está permitindo que ela tenha acesso físico ao dispositivo e, potencialmente, aos seus dados, podendo acessar informações sensíveis, como fotos, mensagens, aplicativos de banco, senhas e outros dados privados. Além disso, há o risco de que a própria pessoa instale aplicativos maliciosos. Também desconfie de promessas milagrosas e pessoas alarmistas, principalmente quando não há transparência sobre os métodos que pretendem utilizar. Você corre o risco de pagar caro por serviços que não entregam o que prometem.

Se precisar de ajuda, procure espaços feministas e transfeministas, que vão saber acolher e ajudar para além das questões meramente técnicas. Na maioria das vezes, o que a gente precisa mesmo é entender melhor os dispositivos que utilizamos, ganhando mais autonomia, tranquilidade e segurança.

Se o que você precisa é apenas reparar algo que não está funcionando bem no seu celular, lembre-se de sempre levar o aparelho para a assistência técnica de sua confiança o mais limpo possível, sem fotos e documentos importantes ou sensíveis. Use a opção de restaurar

mem cis). Isso cria uma dependência que, com o fim da relação, pode se transformar em vulnerabilidade. É daí que nasce o mito do "**meu ex é hacker**": por saber um pouco mais ou ter mais familiaridade com os dispositivos, a pessoa parece ter poderes sobrenaturais sobre as tecnologias. E sobre você.

***Sobre as palavras "hacker" e "hackear"**:*

Gostaríamos de esclarecer que não queremos contribuir para a conotação negativa das palavras "hacker" ou "hackear". Para nós, uma pessoa hacker é alguém curiosa, com habilidades diversas (técnicas ou não), que consegue subverter os sistemas, as normas, os padrões. Seus propósitos podem ser positivos em termos de justiça social — ou exatamente o contrário.

Convidamos a repensar a ideia de "hacker" e "hackear" como algo mais positivo, subversivo e criativo. Vamos parar de reforçar a imagem do hacker como aquele homem-branco-hétero-cis com capacidades técnicas extraordinárias. Nem esses caras têm tantas habilidades, ***nem nós temos tão poucas! Vamos hackear essas ideias!***

2. Sua conta, seu dispositivo e sua linha telefônica não são a mesma coisa!

Quando sentimos que algo estranho está acontecendo com nosso celular, **é comum imaginar que o dispositivo foi hackeado**, ou seja, que o problema esteja no aparelho em si. Mas, na verdade, há diferentes camadas que, se comprometidas, podem afetar a nossa privacidade e segurança no uso do telefone celular. Algumas dessas camadas são: o dispositivo em si e seu sistema operacional, as contas conectadas (como Google ou Apple), e a linha telefônica. Cada um deles tem suas próprias características e consequências. Entender essas diferenças ajuda a reconhecer riscos reais, evitar diagnósticos apressados e buscar soluções mais adequadas com mais tranquilidade e autonomia.

Dispositivo (o celular)

Ter o celular comprometido significa que algum programa malicioso (*malware*) foi instalado no sistema, geralmente com o objetivo de espionar, controlar, roubar dados e dinheiro ou danificar o funcionamento do apa-

É muito improvável / é o menos comum

(mas dependendo do seu perfil, pode acontecer):

- **Ter um software espião altamente sofisticado** (como o *Pegasus*). Se você **NÃO** é jornalista, advogade ou ativista atuando com temas especialmente sensíveis na sua região, é **MUITO provável que você NÃO tenha** um software desse tipo instalado, nem que sue (ex) companheire consiga usar isso para te vigiar. Uma pessoa comum **não tem acesso** a esse tipo de tecnologia, já que ela é vendida apenas para governos e custa MILHARES de dólares[17].

8. Cuidado com supostos hackers e assistência técnica

Quando surge a suspeita de que nosso celular foi hackeado, é comum que a angústia leve a gente a buscar por soluções imediatas. Nesse momento de vulnerabilidade, muita gente acaba recorrendo a supostos hackers ou serviços de assistência técnica duvidosos. O problema é que, em vez de ajudar, essas alternativas podem piorar ainda mais a situação.

17 https://www.elnacional.cat/es/politica/precio-espionaje-pegasus-cuesta-pinchar-movil_760770_102.html

pouco provável que tenham conseguido acessar seus dados.

- Se você tentou instalar um app confiável mas não verificou direito e acabou baixando um app fraudulento, ele pode ser malicioso, acessar seus dados ou exibir publicidade invasiva. Revise com atenção cada app antes de instalar. **Não instale apps fora da Google Play ou Apple Store, a menos que você saiba MUITO BEM o que está fazendo.**

- Se você caiu em um golpe em que alguém se passou por seu banco ou outra empresa confiável e te orientou a instalar um app fraudulento, aí sim pode haver acesso aos seus dados.

- Se você levou seu celular a uma assistência técnica ou pessoa conhecida que se dizia "hacker", ao ter acesso ao aparelho desbloqueado, essa pessoa pode ter visto seus dados, feito cópias ou instalado apps/configurações novas. Sempre que precisar consertar um celular, **leve ele vazio**, use a opção de restaurar para os padrões de fábrica e **não deixe sua conta Google ou Apple logada**.

relho. Existem diferentes tipos de programas que podem ser utilizados para comprometer um celular. Os mais simples possibilitam um acesso ou monitoramento limitado, e geralmente se faz necessário ter o celular-alvo em mãos para instalar. Já os mais sofisticados podem possibilitar acesso amplo ao celular-alvo, no entanto possuem um alto custo, inclusive político, para ser utilizado.

Conta vinculada (Google ou Apple)

Outra camada que pode ser comprometida é a conta Google ou Apple vinculada ao seu celular. Nesse caso, informações sobre o celular podem ser acessadas sem, necessariamente, depender de softwares espiões ou de conhecimentos técnicos muito avançados. Para isso é apenas necessário ter acesso a senha da conta, ou ter acesso a algum dispositivo onde a conta esta ativa. Em contextos íntimos, por exemplo, é muito comum que casais ou familiares compartilhem senhas ou mantenha dispositivos com diversas contas Google ativas. Isso cria uma vulnerabilidade significativa, pois, com acesso à conta, é possível explorar uma série de informações sensíveis e realizar diversas ações, como:

Com acesso à conta do Google, é possível:

→ Rastrear, bloquear ou até apagar o conteúdo do celular remotamente através do "Localizar meu dispositivo";

→ Acessar o histórico de locais visitados (se estiver ativado na sua conta), através do "Histórico de localização";

→ Acessar suas imagens e vídeos armazenados na nuvem através do Google Fotos;

→ Ler seus e-mails e anexos através do Gmail;

→ Acessar os documentos e arquivos armazenados no Google Drive;

→ Acessar compromissos, lembretes e lista de contatos através da Agenda e Contatos;

→ Acessar o histórico de buscas e navegação (se estiver ativado na sua conta);

→ Fazer uma cópia de todos os dados listados acima, de uma só vez, através do Google Takeout;

→ Ter acesso a diversas outras informações atraladas ao uso do celular, como informações sobre o uso dos aplicativos instalados, sendo possível compreender rotinas e hábitos da pessoa; em alguns casos, dados de saúde, histórico de chamadas e SMS, etc.

dos do dispositivo e localizar AirPods, AirTags e outros acessórios compatíveis.

• Se seu (ex) companheire teve acesso físico ao seu celular e algum conhecimento técnico, elu pode ter instalado um app para monitorar sua localização, ativar o microfone, tirar fotos ou espelhar sua tela. A organização feminista Echap mantém uma lista de aplicativos que podem ser usados para essa finalidade[13]. Esses apps costumam se anunciar como ferramentas de controle parental (como o AirDroid Parental Control[14]), anti-roubo (como o Cerberus[15]) ou de suporte técnico remoto (como o AirMirror[16]).

• Se você clicou sem querer em algum link que parecia confiável (SMS, DM em rede social, e-mail etc.), pode ter sido baixado um arquivo malicioso. No entanto, se você não autorizou a instalação a partir de fontes desconhecidas e seguiu os alertas do sistema, é

13 https://github.com/AssoEchap/stalkerware-indicators?tab=readme-ov-file#stalkerware
14 https://play.google.com/store/apps/details?id=com.sand.airdroidkidp
15 https://www.cerberusapp.com/home/pt
16 https://play.google.com/store/apps/details?id=com.sand.airmirror&hl=pt

- **Instalações ou configurações suspeitas após levar o celular a uma assistência técnica** ou alguém que se dizia "hacker", o que pode implicar acesso aos seus dados e até mesmo uma situação de extorsão.

Por exemplo:

- Se seu (ex) companheire teve acesso ao seu celular e configurou o Family Link[10] como se você fosse seu "filhe" > é provável que elu consiga ver sua localização, histórico de localização (se o GPS estiver ativado), suas buscas no Google e Google Maps, além de poder bloquear o celular ou restringir conteúdo e apps.

- Se seu (ex) companheire acessou sua conta Google ou Apple, elu pode ativar funcionalidades de localização como o Buscar[11] no iOS ou o Buscar meu dispositivo[12] no Android > se a localização estiver ativada, é provável que elu possa ver onde seu celular está. No entanto, quando ativado, o celular emite um som e um aviso. Essa função também permite apagar os da-

10 https://families.google/intl/pt-BR/familylink/
11 https://www.apple.com/br/icloud/find-my/
12 https://www.google.com/android/find/about?hl=pt-BR

Com acesso à conta do Apple, é possível:

→ Localizar, bloquear ou apagar o dispositivo através do "Buscar iPhone"; Acessar fotos e vídeos salvos no iCloud;

→ Acessar e-mails vinculados ao iCloud Mail;

→ Acessar backups do iPhone, que podem incluir mensagens do iMessage, dados de apps e até do WhatsApp (se houver backup via iCloud);

→ Notas, contatos, calendário, lembretes, etc;

→ Download completo de dados via ferramentas da Apple.

Linha telefônica comprometida

Ter a linha telefônica comprometida é diferente de ter o celular ou uma conta invadida. Podemos considerar que uma linha telefônica foi comprometida de duas formas principais, através de uma técnica chamada SIM swap, ou através de interceptação telefônica.

SIM swap

Ocorre quando alguém consegue **transferir seu número de telefone para outro chip**, sem que você autorize. Para isso, a pessoa geralmente se passa por você jun-

to à operadora, usando dados pessoais, e solicita a substituição do chip. Com acesso a sua linha, a pessoa passa a receber suas mensagens SMS e ligações, e pode, com isso, receber códigos e acessar sua conta do Whatsapp, Signal, Telegram. Além de ser possível também invadir contas de email e redes sociais através de recursos como "esqueci a senha".

Interceptação telefônica (grampo)

Ocorre quando alguém passa a **interceptar o conteúdo das suas comunicações telefônicas**. Ou seja, a partir do momento que seu número é grampeado, o conteúdo de suas ligações feitas através da linha telefônica passa a ser gravado. O conteúdo dos SMS enviados e recebidos também são interceptados. Além disso, Informações de geolocalização também podem ser acessadas em tempo real. Note que aqui estamos falando de comunicações realizadas através da rede de telefonia, e não de Internet.

A interceptação telefonica pode ser feita de maneira **legal**, através do sistema de justiça, dentro de uma investigação policial; ou de forma **ilegal**, utilizando, muitas vezes, equipamento clandestino, ou mesmo corru-

lento, os apps fechem sozinhos, a bateria acabe rápido ou o celular funcione de forma estranha.

Pode acontecer:

- **Uso de funcionalidades de controle parental** (como o Family Link do Google[9]) para te localizar, ver buscas no Google Maps, histórico de localização, buscas do Google ou até bloquear o celular.

- **Uso da funcionalidade "buscar meu dispositivo"** para te localizar.

- **Uso de aplicativos espiões**, embora seja necessário ter tido acesso ao celular por tempo suficiente para instalar e configurar o app.

- **Instalação de apps fraudulentos ou vírus**, sem que isso signifique que sue (ex) companheire tenha controle do seu celular.

- **Cair em golpes que induzem à instalação de apps fraudulentos**, que podem dar acesso aos seus dados a golpistas.

9 https://families.google/intl/es/familylink/

ba sua senha e possa acessar de outro dispositivo. O mesmo vale para sua conta Apple no iPhone.

- Se você usa a mesma senha para todas as contas e já compartilhou com sue (ex) companheire > o mais provável é que elu saiba a senha e possa acessar suas redes sociais ou contas Google/Apple de outro dispositivo.

- Se sue (ex) companheire tem acesso a dispositivos (celular, laptop, TV etc.) onde sua conta Google está logada > o mais provável é que esse acesso seja feito através da conta Google.

- Se sue celular está velho, danificado ou tem poucos recursos > o mais provável é que ele fique lento, descarregue rapidamente ou apresente comportamentos estranhos.

- Se você está usando o celular mais que o habitual por causa do estresse > o mais provável é que a bateria acabe mais rápido.

- Se há muitos aplicativos instalados e o armazenamento está quase cheio > o mais provável é que fique

pção de funcionários. Esse tipo de interceptação é crime em diversos países, e pode violar direitos constitucionais.

Portanto, **dependendo do caso, a abordagem será diferente**; nesta tabela, apresentamos um resumo:

O que eu acho que foi hackeado?	**O que eu poderia fazer para impedir isso?**
Dispositivo (celular)	Verificar se há um programa malicioso (*malware*) no dispositivo; verificar os aplicativos instalados e as permissões; verificar os aplicativos e as funcionalidades de controle parental; executar uma redefinição de fábrica (todos os dados serão perdidos); substituir o dispositivo.
Conta vinculada (Google ou Apple)	Alterar as senhas e os métodos de recuperação de conta; revisar as sessões conectadas
Linha telefônica	Trocar de número (chip); evitar fazer ligações e enviar SMS, e fazer chamadas via WhatsApp ou Signal (que não usam a linha telefônica, mas a Internet); remover o número grampeado dos métodos de recuperação de contas ou da autenticação de dois fatores.

*Muitas pessoas que sentem que foram hackeadas têm o impulso de **mudar seu número de telefone (chip)**, acreditando que isso implica uma mudança total da vida digital, mas não é esse o caso. **A troca de chip não impede o acesso a uma conta** do Google ou da Apple, **nem remove um possível software espião** ou aplicativo de controle parental. Esperamos que essas informações o ajudem a entender melhor e a orientar suas ações futuras.*

3. E como funcionam os programas espiões?

Quando falamos em celular hackeado é comum pensar na palavra *malware*. Esse é um nome genérico para programas maliciosos criados com o objetivo de causar danos, roubar informações ou espionar dispositivos. Existem diferentes tipos de *malware*, como por exemplo: Vírus, *Worms*, *Trojans*, *Adware*, *Ransomware*, RATs, *Spyware*. A lista é extensa, e muitas vezes é possível que haja diferentes tipos em um só programa. Mas vale a pena chamar atenção para os software espião, que são utilizados com o objetivo de coletar informações sem o conhecimento ou consentimento da pessoa-alvo. Ou seja, são construídos na intensão de serem silenciosos, coletando

O mais provável / o mais comum:

- **Acesso à contas do Google, Apple ou redes sociais sem métodos muito técnicos**, seja porque a senha foi compartilhada, porque é uma senha fácil de adivinhar, porque usa a mesma para todas as contas, porque a conta continua logada em algum dispositivo anteriormente compartilhado, ou porque têm filhes em comum que podem fornecer a senha ou usam celulares com suas contas logadas. Ou seja, acesso por descuido, uso da tecnologia com poucas medidas de proteção, brecha digital, etc.

- **Funcionamento lento/estranho do celular ou descarga rápida da bateria**, porque é antigo, tem poucos recursos, muitos aplicativos instalados e está sendo mais usado em um momento de estresse.

- Notificações de publicidade invasivas**, muito comuns em fabricantes chineses, como a Xiaomi.

Por exemplo:

- Se sue (ex) companheire configurou sua conta do Google no seu celular > o mais provável é que elu sai-

to usando o site *virustotal.com*, ou pesquisando a mensagem que recebeu na internet.

- **O app Malwarebytes detectou algo suspeito**: o Malwarebytes[7] é uma ferramenta confiável para escanear celulares. Você pode usar a versão de teste para analisar seu dispositivo. Se ele identificar algum app potencialmente malicioso, peça ajuda[8]. Cuidado com outros antivírus para celular, muitos são cheios de propaganda invasiva e alguns podem até ser maliciosos!

7. O que pode ter acontecido?

Queremos te mostrar aqui uma lista de possíveis situações e o quão comuns/prováveis elas são, com base na nossa experiência trabalhando com linhas de apoio feminista. Uma das linhas que entrevistamos chamava essa classificação de **"pirâmide de probabilidade"**.

Esperamos que te ajude a ter uma ideia do que pode ter acontecido, mas tudo depende do seu caso e contexto!

7 https://www.malwarebytes.com/pt/
8 Consulte a seção 9.

dados da forma mais imperceptível possível. Existem software espião mais simples, como os utilizados em contextos de relacionamentos abusivos, por exemplo, e outros mais sofisticados, como os utilizados por governos.

Software espiõe usados em relações afetivas
(em inglês, Spouseware o Stalkerware)

São software espião mais simples e acessíveis. Geralmente são anunciados como ferramentas de controle parental, e podem ser adquiridos por um baixo custo ou de forma gratuita. Para ser instalado, é preciso que alguém tenha acesso direto (fisicamente) ao celular-alvo, e saiba exatamente o que fazer, já que é muito raro ter esses programas disponíveis em lojas como PlayStore ou AppStore e, além de instalar, muitas vezes é preciso fazer algumas configurações. Outra possibilidade é que ele seja enviado através de um link malicioso, de forma a enganar a pessoa para que clique e baixe o app. Nesse caso, o celular costuma pedir autorizações, como permitir acesso à localização, câmera, ou mensagens. Ou seja, haveria sinais, mesmo que sutis.

Software espião sofisticados

Além dos softwares espiõe usados em relações afetivas, existem também softwares espiõe altamente sofisticados, desenvolvidos por empresas especializadas em vigilância digital e, em geral, utilizados por governos em contextos específicos. Esses programas costumam explorar falhas de segurança ainda desconhecidas (vulnerabilidade de dia zero[1]) e, em alguns casos, conseguem acessar um dispositivo sem que a pessoa clique em nada. Um exemplo é o Pegasus, software que ganhou notoriedade por ter sido utilizado de forma abusiva para monitorar jornalistas e ativistas. Esse tipo de tecnologia, no entanto, possui um custo muito elevado e não é utilizada de forma massiva ou indiscriminada. São ferramentas direcionadas e aplicadas em contextos muito específicos e, por isso, não representam um risco real para o coti

Registrador de teclas (em inglês, *Keylogger*)

São programas maliciosos projetados para capturar e registrar cada tecla pressionada no teclado de um dispositivo, monitorando tudo o que é digitado. Eles podem

1 https://pt.wikipedia.org/wiki/Vulnerabilidade_de_dia_zero

acesso ao microfone, câmera, localização ou acessibilidade. Se tiver dúvidas, peça ajuda[5] para revisar seus apps.

- **O Google Play Protect está desativado**: esse é um recurso da PlayStore que ajuda a impedir a instalação de apps maliciosos. Se estiver desativado, isso não é um bom sinal. Você pode verificar o status dele consultando a documentação oficial do Google[6].

- **A opção "Instalar apps desconhecidos" está ativada para algum navegador ou gerenciador de arquivos**: isso permite que aplicativos sejam instalados sem passar pela Play Store, ou seja, sem verificação de segurança, e pode ser uma porta de entrada para apps maliciosos.

- **Você clicou em um link sem verificar muito bem**: se você recebeu uma mensagem que parecia confiável e acabou clicando no link, mantenha a calma, isso pode acontecer com qualquer pessoa. Mas fique atente e verifique se algum app foi baixado ou instalado nesse processo. Você pode verificar se o link é suspei-

5 Consulte a seção 9.
6 https://support.google.com/android/answer/2812853?hl=pt

nas) de pedidos de seguidores, isso acontece o tempo todo na internet. Através de uma solicitação de seguidor não é possível invadir sua conta nem seu celular.

- **"Pessoas desconhecidas me mandaram mensagens no WhatsApp ou redes sociais"**: há tentativas em massa de iniciar conversas nesses canais. Muitas vezes são golpes, ou apenas tentativas de verificar se um número existe. Você pode bloquear, denunciar ou simplesmente não responder.

Agora, veja alguns **sinais que de fato merecem atenção**:

- **Você encontra aplicativos novos que não reconhece**: mas calma, não se assuste logo de cara. Muitos apps do sistema são pouco conhecidos, mas são legítimos e necessários para o funcionamento do celular. Se tiver dúvidas, pesquise na internet o nome do app que te parece suspeito. Duas boas referências para isso são: *immuniweb.com* e *reports.exodus-privacy.eu.org*. Você também pode procurar o nome do aplicativo em qualquer buscador para entender do que se trata. Preste atenção especial nos apps que têm

ser utilizados para roubar senhas, dados bancários, monitorar comunicações privadas, etc. Em celulares, podem estar presentes em aplicativos de teclado alternativos, ferramentas de controle parental, software espiõe usados em relações afetivas ou aplicativos que abusam de serviços de acessibilidade, permitindo ler texto em campos sensíveis.

4. Apps para proteger ou para controlar?

Aplicativos criados para controle parental, como Google Family Link, Life360 ou apps de rastreamento, têm sido cada vez mais **usados em relações afetivas como ferramentas de controle e vigilância**. Vendidos sob a narrativa da segurança e proteção familiar, muitos desses apps acabam sendo usados por companheires para **monitorar localização, histórico de chamadas, redes sociais e até tempo de tela, sem consentimento**.

Além dos apps mais conhecidos, existe também um mercado silencioso de softwares espiões usados em relações afetivas que se disfarçam como ferramentas de controle parental, mas foram claramente projetados

para serem utilizados no contexto de relações afetivas. Muitos desses aplicativos podem ser encontrados facilmente na web, não em lojas oficiais como a PlayStore, mas em sites próprios, com aparência profissional, oferecendo "monitoramento familiar", "rastreamento de funcionários" ou "proteção de entes queridos".

A linha entre proteção e controle é tênue. Em qualquer relação, seja com filhes ou parceires, é natural querer proteger quem se ama. Mas há uma diferença fundamental entre cuidar e controlar. Quando o cuidado se transforma em vigilância sem consentimento, quando o zelo se apoia na desconfiança, o que era proteção pode rapidamente se tornar violência.

5. Seguramente não é hacker

Companheire, achamos importante que você tenha esta informação. Talvez sue companheire ou ex-companheire tenha dito que era hacker ou que conhecia hackers, talvez tenha feito você acreditar que elu entende muito de tecnologia e é capaz de "hackear" dispositivos "como num passe de mágica". A realidade é que não é bem assim.

- **"Meu celular está lento"**: se ele tem muitos apps abertos, já é um modelo mais antigo e não tem muita capacidade... é normal que fique lento.

- **"Recebo notificações estranhas"**: alguns telefones de fabricantes chineses (como a Xiaomi) trazem muita publicidade em seus aplicativos. Essa publicidade às vezes é bem invasiva e aparece como notificações. Verifique a configuração dos seus apps e das notificações. Se continuar recebendo alertas que não parecem vir de nenhum app instalado e você não conseguir desativar, aí sim vale buscar ajuda[4].

- **"Recebi alertas de vírus no navegador"**: o mais provável é que você tenha acessado um site que exibe alertas falsos de vírus para te assustar e te fazer clicar. A intenção geralmente é maliciosa. Não clique em nenhum alerta, mesmo que pareçam reais, é fácil se confundir. Esse tipo de golpe é, infelizmente, comum na internet.

- **"Recebi solicitações de seguidores nas redes sociais"**: é comum recebermos dezenas (ou até cente-

4 Consulte a seção 9.

6. Quais sintomas são preocupantes e quais não são

Em uma situação de estresse e angústia, **é muito comum ficarmos em estado de alerta e prestar mais atenção ao comportamento dos nossos dispositivos**. É parecido com quando enfrentamos algum problema de saúde: começamos a observar mais o nosso corpo e, de repente, percebemos sintomas novos, sem saber se já estavam ali antes, há quanto tempo ou se têm alguma relação com o que estamos sentindo.

Aqui estão alguns sintomas que você pode começar a observar, mas que sozinhos **NÃO são motivo de preocupação**:

- **"Sinto que a bateria do meu celular está descarregando muito rápido"**: provavelmente seu celular já tem mais de dois anos, tem muitos apps instalados, e nesses dias de estresse você tem se comunicado mais com suas pessoas queridas e usado bastante as redes sociais, tudo isso faz com que a bateria acabe mais rápido.

A ideia de "hacker" que temos na cabeça é apenas uma ficção, coisa de cinema. Mas que, no entanto, atua no nosso imaginário e nos faz pensar que alguém com conhecimentos extraordinários pode violar os sistemas de proteção dos nossos dispositivos. A verdade é que, para que um dispositivo ou aplicativo chegue ao mercado, ele precisa passar por muitos controles de segurança antes de cair nas suas mãos. Existem equipes de pessoas que trabalham diariamente para garantir isso. Quando uma vulnerabilidade de segurança é identificada, atualizações são lançadas imediatamente para corrigi-la.

Por mais que sue (ex)companheire tenha estudado computação, passe muitas horas no computador ou diga que é "expert" no assunto:

- **Elu não pode acessar seu dispositivo remotamente "como num passe de mágica"**. Para isso, teria que ter tido acesso físico ao celular e instalado algum aplicativo com essa finalidade. Pense se essa pessoa teve acesso físico ao seu celular, com tempo suficiente para instalar algum app. Se sim, você pode revisar os

aplicativos instalados ou pedir ajuda para fazer uma verificação no seu celular[2].

- **Elu não pode acessar suas contas se não tiver como descobrir sua senha** ou se a conta não tiver permanecido ativa em algum dispositivo que você possa ter compartilhado com essa pessoa. Se estiver em dúvida: fortaleça suas senhas e revise as sessões ativas. Se precisar, você pode buscar ajuda em uma linha de atendimento feminista para te acompanhar nesse processo[3].

Além disso, queremos te contar que, na maioria das vezes em que alguém diz ser "hacker", o que essa pessoa faz é usar:

- **Técnicas de engenharia social**, ou seja, diferentes formas de influenciar, manipular ou enganar para que a pessoa acabe compartilhando senhas ou códigos de segurança. Pode, inclusive, usar familiares, amigues ou filhes em comum para conseguir essas informações.

2 Consulte as seções 9 e 10.
3 idem

- **Fontes abertas e dados disponíveis na internet** para obter informações pessoais e até simular que teve acesso a dispositivos, quando na verdade apenas pesquisou esses dados online.

Cuidado com os e-mails de recuperação de conta! *Não é preciso saber muito para clicar em "esqueci a senha" no Instagram, Facebook ou qualquer outra rede social e fazer com que um link de redefinição seja enviado ao e-mail de recuperação. Se esse e-mail for antigo, você não acessa com frequência, está com uma senha fraca ou foi compartilhado com sue (ex)companheire... então elu pode facilmente acessar e trocar a senha da sua conta. Essa é uma forma bastante comum de acesso indesejado e sequestro de contas por parte de familiares ou ex. Lembre-se de manter seu e-mail de recuperação atualizado e protegido com uma boa senha.*