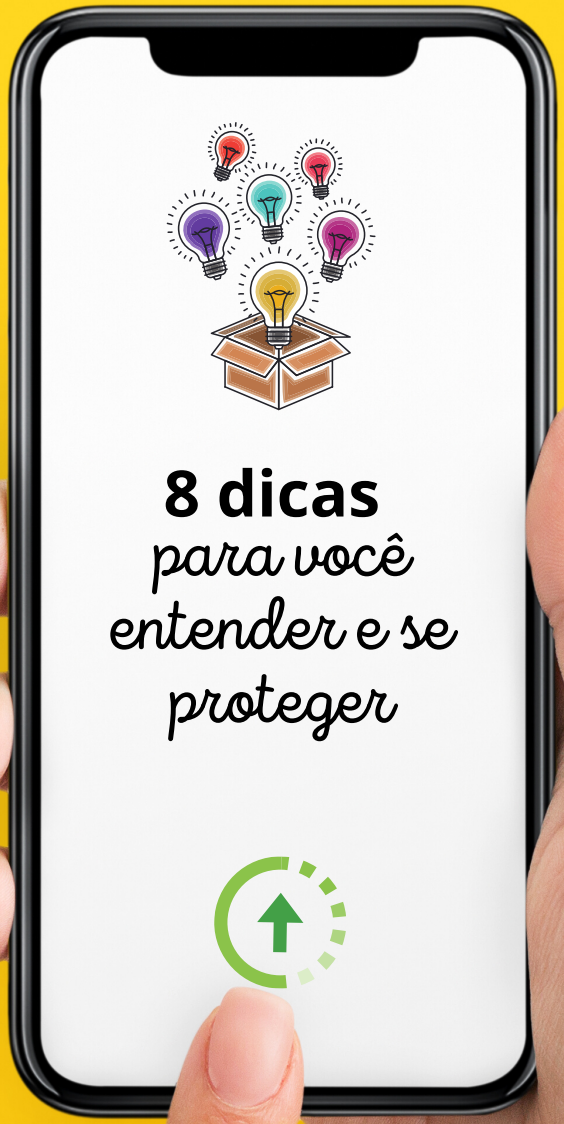
Segurança Digital



1

2

3

4

5

6

7

8

Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO
E PESQUISA EM INOVAÇÃO

Produção em parceria

placamae.org_

FGV DIREITO SP
CENTRO DE ENSINO
E PESQUISA EM INOVAÇÃO

Projeto gráfico e Editoração
Paloma Mendes Saldanha
PlacaMãe.Org_

Autores

Aline Taraziuk Nicodemos
Guilherme Forma Klafke
Paloma Mendes Saldanha
Stephane Hilda Barbosa Lima
Tatiana Guimarães

VOCÊ TEM O DIREITO DE:
Compartilhar, copiar e redistribuir o material em qualquer suporte ou formato de acordo com os seguintes termos:

ATRIBUIÇÃO
Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de maneira alguma que sugira ao licenciante a apoiar você ou o seu uso.

USO NÃO COMERCIAL
Você não pode usar o material para fins comerciais.

SEM DERIVAÇÕES
Se você remixar, transformar ou criar a partir do material,você não pode distribuir o material modificado.

Creative Commons
Atribuição-NãoComercial
SemDerivações 4.0 Internacional

1 Pare e reflita!

A dica de PARAR E REFLETIR serve para que você pense e entenda que não precisa ir na velocidade da internet e que você deve questionar tudo o que chega até você.

- Preciso compartilhar?
- Por qual motivo aquilo chegou até mim?
- Preciso responder agora?

As ofertas de compras na internet , por exemplo, são constantes e extremamente variadas. Mas o que você faz quando aparece, numa rede social, a oferta de compra de algo que lhe interessa?

- [ ] Clica, preenche o formulário com seu nome, CPF, cartão de crédito etc. e finaliza o pedido.
- [ ] Faz a consulta nos buscadores, como o Google, por exemplo, sobre a pessoa que está vendendo e sobre como aquelas vendas estão ocorrendo com outras pessoas.

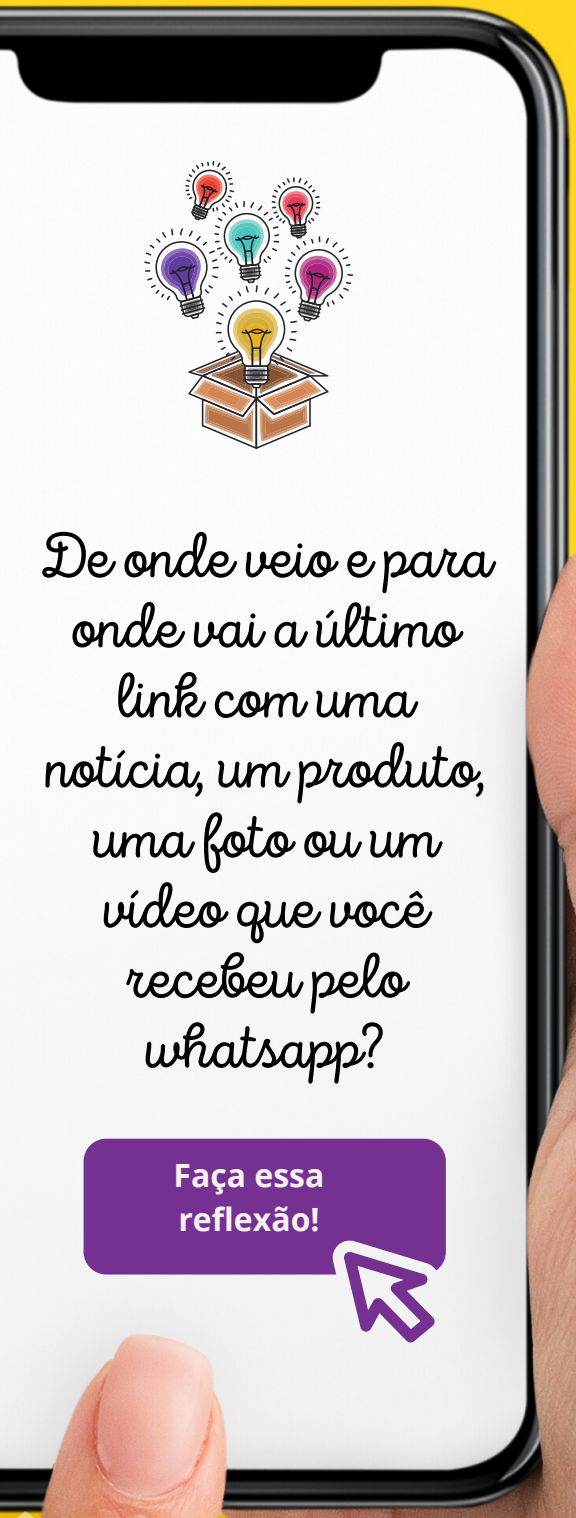
Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

De onde as coisas vêm e para onde elas vão?

2



A gente tem a mania de reagir a todo instante e a tudo como se todas as informações que chegam até nós fossem verdades incontestáveis. Mas você já parou para pensar de onde as informações vêm e para onde elas vão?

- ☐ Sim
- ☐ Não
- ☐ As vezes sim

Quem produz a informação tem um interesse e, as vezes, esse interesse consiste em manipular a verdade. E aí você começa a defender uma ideia errada e com o objetivo de mascarar o que de fato aconteceu.

62% dos brasileiros não conseguem reconhecer uma notícia falsa. Essa foi a conclusão chegada pela pesquisa "Iceberg digital" desenvolvida pela Kaspersky em parceria com a CORPA.

Não seria melhor fazer algumas perguntas antes de aceitar as informações que chegam até você?

- Quem fez essa notícia, foto ou vídeo?
- Qual foi o público-alvo?
- Existem erros de português no texto?
- Por qual motivo o conteúdo é anônimo?

Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

3 Tenha consciência do seu comportamento na internet

Sabia que ter consciência do seu uso e comportamento digital faz parte do plano "estar protegido digitalmente"?

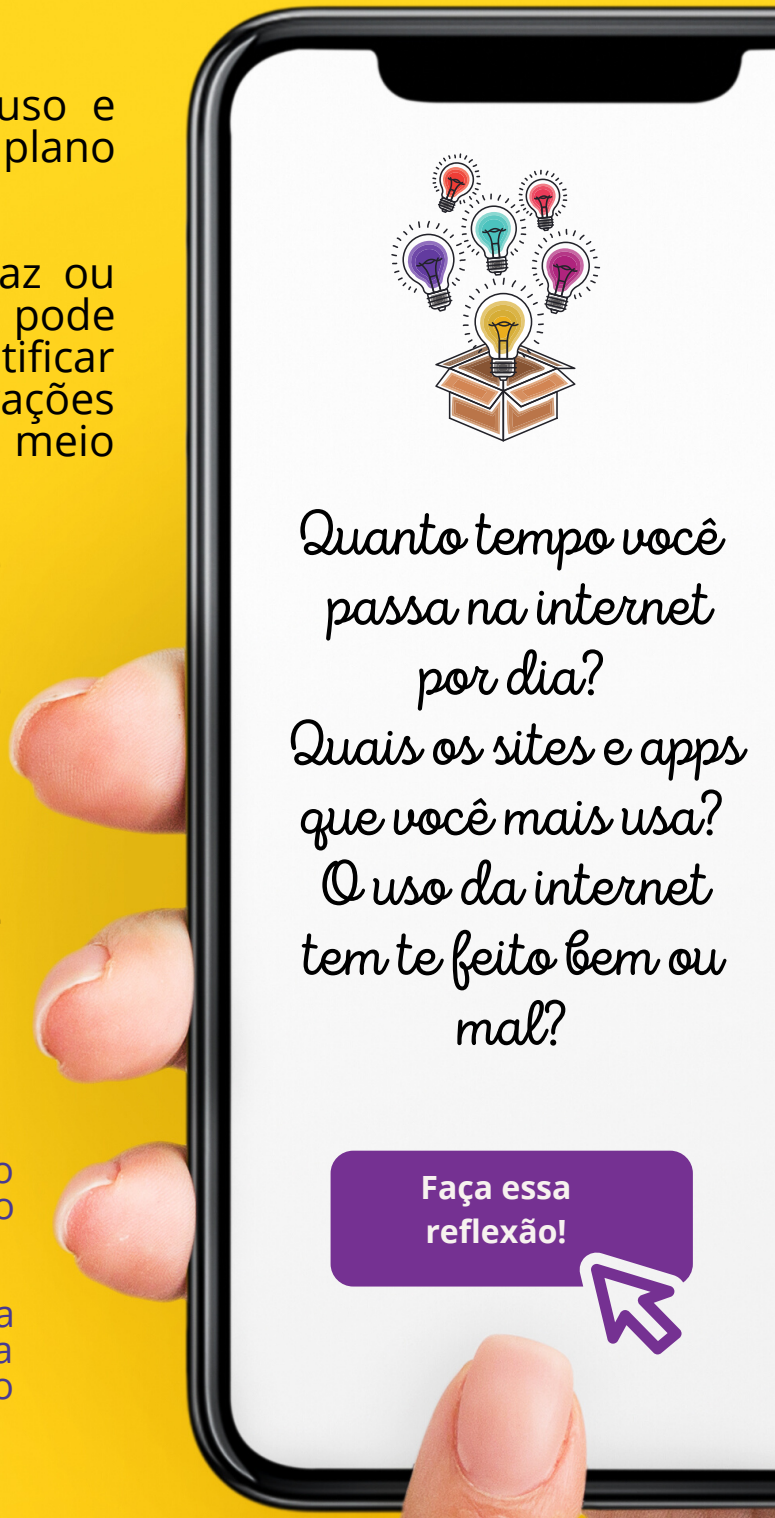
Ao saber exatamente o que você faz ou deixa de fazer na internet, você pode melhorar o seu bem-estar e identificar com mais facilidade algumas alterações maliciosas que podem acontecer no meio ambiente digital.

Para quem tem um smartphone ANDROID, pode gerenciar o uso do seu aparelho por meio do "Bem-estar digital". Olha como você pode configurar:

1. Abra o app Config. do smartphone;
2. Toque em Bem-estar digital e controle dos pais;
3. Em "Suas ferramentas do Bem-estar digital", toque em Mostrar seus dados.

Obs.1: Na 1ª vez que você abrir o Bem-estar digital, será necessário configurar seu perfil.

Obs.2: Você pode gerenciar a conta de uma criança caso sua conta seja a de pai/mãe padrão no dispositivo dela.

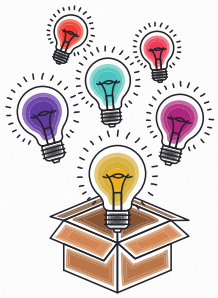


Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

Segurança tem que ser física e digital



Você já deixou seu computador aberto numa mesa de reunião enquanto ia ao banheiro, por exemplo?
Ao finalizar o uso de um app no computador você desloga ou só clica no "X" para fechar a janela?

Faça essa reflexão!

A internet não está ligada unicamente ao que é digital. Para fazer o digital funcionar a gente precisa de um suporte físico. São o que chamamos de dispositivos ou gadgets. Ex.: smartphone, televisão, relógio, computador etc. E por isso é tão importante a gente pensar na segurança como algo mais amplo que só o ambiente digital.

Pensando nisso, olha as dicas de apps que colocam senha nos aplicativos do seu smartphone:

App Lock (Android)
Bloqueio (Android)
Norton App Lock (Android)
Family Time (IOS)

E antes de acessar uma rede pública de wi-fi, analisa no app McAfee Mobile Security se aquela rede é segura.

Ah! outra coisa que queríamos te perguntar: Você compartilha sua senha pelo whatsapp, e-mail ou qualquer outro item do meio ambiente digital?

Se sim, volta nas dicas 1 e 2 !

Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

5 Senhas: como criá-las?

Como a gente já disse, segurança não é só senha, mas é muito importante que a gente saiba criá-la de maneira a preservar o nosso espaço.

Presta atenção:

- Não anote a senha e a deixe exposta (post-it, por exemplo);
- Não compartilhe sua senha pela internet;
- Não use informações pessoais para construir sua senha;
- Evite ter a mesma senha para todas as contas;
- Evite sequências na criação da senha;
- Use programas para gerar e armazenar senhas;
- Altere sua senha a cada 3 meses.

Dicas de como criar senhas fortes

1. Use letras, números e símbolos;
2. Intercale letras maiúsculas e minúsculas;
3. Use mais de 8 caracteres.

Exemplos

Crie uma frase base e utilize as letras iniciais de cada palavra para servir de senha e incremente com as dicas acima.

Eu **a**mo **e**studar **D**ireito **D**igital.

→ Ea3Dd#001

OU

George Clooney → G3oR93c10oN3y

Que tal trocar suas senhas hoje?

Faça essa reflexão!

10 piores senhas de 2019

Segundo os serviços de cibersegurança SplashData

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

Parceria

placamae.org

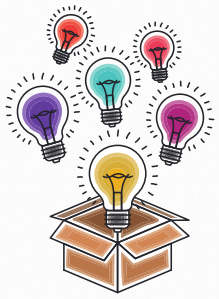
FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

6 Ataques maliciosos

Aqui a dica envolve ações de terceiros. Então é necessário ficar alerta para saber decidir quais são as informações sensíveis que você não gostaria que sofresse um ataque malicioso. Prestar atenção ao que aparece em nossa tela é muito importante para não cairmos em golpes na internet.

Faça esse check list e reflita:

- ☐ Meus programas e apps estão atualizados?
- ☐ Deletei os apps e softwares que não uso?
- ☐ Utilizo sites e plataformas oficiais para fazer download?
- ☐ Minhas senhas são fortes como sugere a dica 5?
- ☐ Acionei o duplo fator de autenticação do whatsapp, do email etc.?
- ☐ Utilizo conexões seguras para acessar a internet?
- ☐ Utilizo firewall e antivírus confiáveis e atualizados?
- ☐ Fiz backup dos meus arquivos?
- ☐ Eu solicitei algum boleto a ser enviado pelo email ou por link?
- ☐ Repassei senha de banco e de redes sociais pela internet?



Você sabia?

PHISHING são sites e aplicativos que se passam por empresas ou pessoas famosas, com o intuito de enganar os usuários para obter informações confidenciais, como senhas bancárias, de e-mail e redes sociais ou, então, tentam persuadir o usuário a realizar determinadas ações.

Pesquise também a definição de Spyware, Trojan, Rootkit e Worm. Vale a pena se informar!

Faça essa reflexão!

Parceria

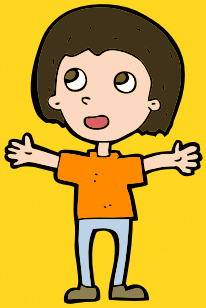
placamae.org_

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

Compartilhamento de conteúdo

Cuidado com a superexposição, ou seja, cuidado com o compartilhamento excessivo de fotos, de informações de localização etc. Nesta dica, o importante é perceber quando aquele compartilhamento vai gerar ou não um risco para você.

Quem pode ver? Qual é o conteúdo que estou postando? Em qual rede social estou postando ? Pessoal ou profissional? Perfil público ou privado?



- Revise e configure as opções de privacidade em todas as suas redes sociais;
- Pense no que quer que os outros vejam.

Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

O que fazer?

Sofri um ataque malicioso e roubaram meus dados; Compartilharam minha foto com dizeres inapropriados; pegaram meu vídeo e o descontextualizaram ; etc.
E agora?

1) Converse com alguém de confiança

Não faça nada sozinho(a). Chame alguém de confiança e que possa te ajudar.

2) Não apague as provas.

Faça prints do que foi divulgado, registre a data de acesso e o link da página onde o conteúdo foi divulgado. Também pode fazer uma impressão em PDF, gravar vídeos etc. Tudo que possa documentar o incidente.

3) Registre um Boletim de Ocorrência.

Existe uma delegacia especializada em crimes cibernéticos em Recife (Endereço: Rua da Aurora, 487 - Boa Vista, Recife – PE). Procure a delegacia, especializada ou não, da sua cidade e relate o que houve registrando o B.O.

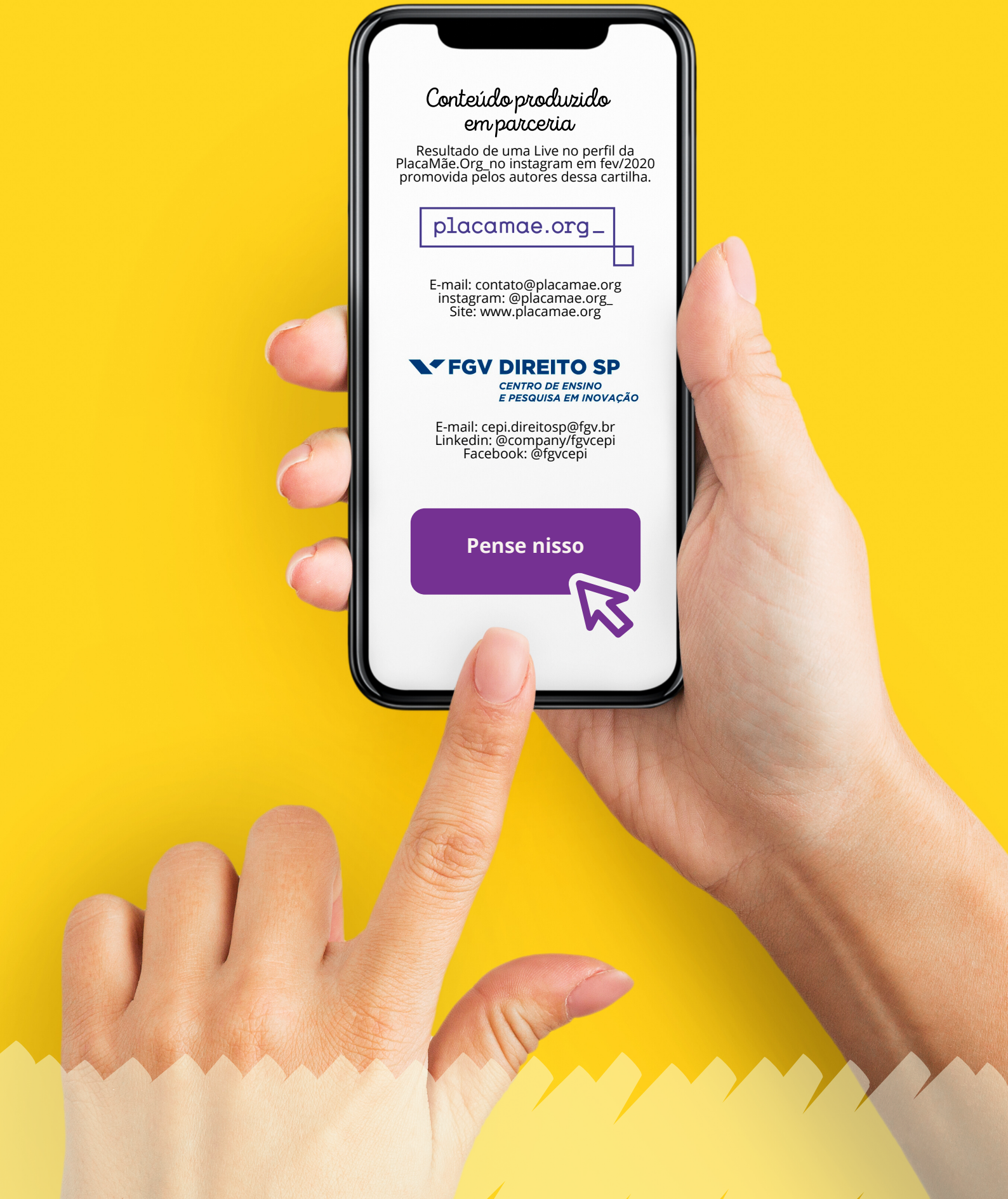
4) Faça uma ata notarial.

No caso de compartilhamento não autorizado de foto ou vídeo. A ata poderá ser realizada em qualquer cartório de notas, desde que as provas sejam levadas até o tabelião, o qual irá descrever o fato que passará a ser verdadeiro para todos os efeitos, em juízo ou fora dele. Não tendo condições financeiras para solicitar uma ata notarial, o print da tela conforme o ponto 1 pode ser utilizado num processo judicial. O que não pode é não documentar a sua prova.

Parceria

placamae.org

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO


Conteúdo produzido em parceria
Resultado de uma Live no perfil da PlacaMãe.Org_no instagram em fev/2020 promovida pelos autores dessa cartilha.
placamae.org_
E-mail: contato@placamae.org
instagram: @placamae.org_
Site: www.placamae.org
FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO
E-mail: cepi.direitosp@fgv.br
Linkedin: @company/fgvcepi
Facebook: @fgvcepi
Pense nisso