Centro Universitário Processus

PORTARIA Nº 282, DE 14 DE ABRIL DE 2022

CENTRO UNIVERSITÁRIO PROCESSUS
Atividade Extensionista
RELATÓRIO FINAL (2023.2)

CURSO: GRADUAÇÃO EM DIREITO / DIREITO DIGITAL / CAMPUS DA ASA SUL / TURNO: NOTURNO
TÍTULO DO PROJETO/AÇÃO: PREVENÇAO AOS CRIMES CIBERNÉTICOS
PERÍODO DE EXECUÇÃO:
Data Início: 08/2023 **Data Término:** 12/2023
EQUIPE:
Nome completo **Curso/matrícula**
Rosalina Gonçalves da Cunha Matrícula| 1910010000011 | Direito Digital (Direito / Asa Sul / Noturno)
Caroline Batistella| 920010000046 | Direito Digital (Direito / Asa Sul / Noturno)
Marcello Carvalho de Araujo | 2210010000084 | Direito Digital (Direito / Asa Sul / Noturno)
Vanderlei Flores de Oliveira| 2010010000263 | Direito Digital (Direito / Asa Sul / Noturno)
João Pedro Mendes de Souza| 2020010000076 | Direito Digital (Direito / Asa Sul / Noturno)
Iris Portela Gomiero| 1910010000131 | Direito Digital (Direito / Asa Sul / Noturno)
Erivelto Drumond Ponte| 1920010000096 | Direito Digital (Direito / Asa Sul / Noturno)
Kallel Filipe dos Santos Araújo | 2310010000020 | Direito Digital (Direito / Asa Sul / Noturno)
Gabrielly Ogawa de Abreu | 2310010000083 | Direito Digital (Direito / Asa Sul / Noturno)
PROFESSOR (A) ARTICULADOR (A) (orientador (a)):
Prof. Dr. Henrique Savonitti Miranda
INSTITUIÇÃO PARCEIRA:
Não houve.
PÚBLICO-ALVO: População brasileira
RESUMO: Os projetos de extensão universitária buscam criar um vínculo entre a instituição de ensino superior e a sociedade na qual ela está inserida, de modo a possibilitar a propagação de conhecimentos adquiridos na formação acadêmica. Tornam-se, desse modo, um ambiente que

possibilita vivências entre instituição e as reais necessidades dos indivíduos. O presente projeto extensionista objetiva analisar os crimes cibernéticos com foco na obtenção de ganhos financeiros, bens ou divulgação de informações pessoais obtidas ilegalmente pelos criminosos. Isso é alcançado através da ameaça como meio de coerção. Além disso, objetivamos apresentar relatos que evidenciem a prática da extorsão cibernética, destacar os perigos associados a esse crime, discutir medidas de prevenção, detalhar o processo que leva à concretização do crime, identificar os tipos de ameaças utilizadas pelos criminosos e, se o crime for concretizado, abordar as estratégias para minimizar os danos. O enfoque principal está nos golpes de extorsão realizados via WhatsApp e no uso de spyware como ferramenta para essa prática delituosa.
RESULTADOS ESPERADOS: O plano de ação para conscientização da população sobre golpes de extorsão e espionagem cibernética inclui a criação de uma cartilha informativa que será distribuída pelo grupo, nas ruas de Brasília. Nessa cartilha, serão compartilhados alertas e orientações sobre os principais golpes de extorsão e métodos de espionagem em dispositivos eletrônicos e internet. A estratégia envolve a produção de conteúdo educativo e a promoção de conscientização digital por meio da distribuição da cartilha.
Quantidade de beneficiários (estimativa)
Mais de 300 beneficiários. (estimativa pela quantidade de cartilhas distribuídas).

Observações:

Não há.

ANEXOS AO RELATÓRIO:

I – Projeto extensionista (Arquivo: Projeto);

II – Pesquisa realizada pelos alunos na fase de preparação (Arquivo: Desenvolvimento do tema);

III – Exposição do tema pesquisado para os colegas de classe (Arquivo: Internalização);

IV – Relatório contendo os resultados obtidos na atividade extensionista (Arquivo: Resultados Alcançados);

V – Relatório fotográfico das atividades (Arquivo: Relatório fotográfico)

VI – Fotos dos trabalhos desenvolvidos em sala e das atividades extensionistas desenvolvidas (assim como os documentos acima, inseridas na área de "Registros" do Projeto na plataforma SPGAEX).

Henrique Savonitti

Professor(a) articulador(a)

Coordenador(a) de Extensão

Coordenador(a) de Curso


ESTELIONATO ELETRÔNICO

PROF. DR. HENRIQUE SAVONITTI MIRANDA

Caroline Batistella

Erivelto Drumond Ponte

Iris Portela Gomiero

João Pedro Mendes de Souza

Kallel Filipe dos Santos Araújo

Marcello Carvalho de Araújo

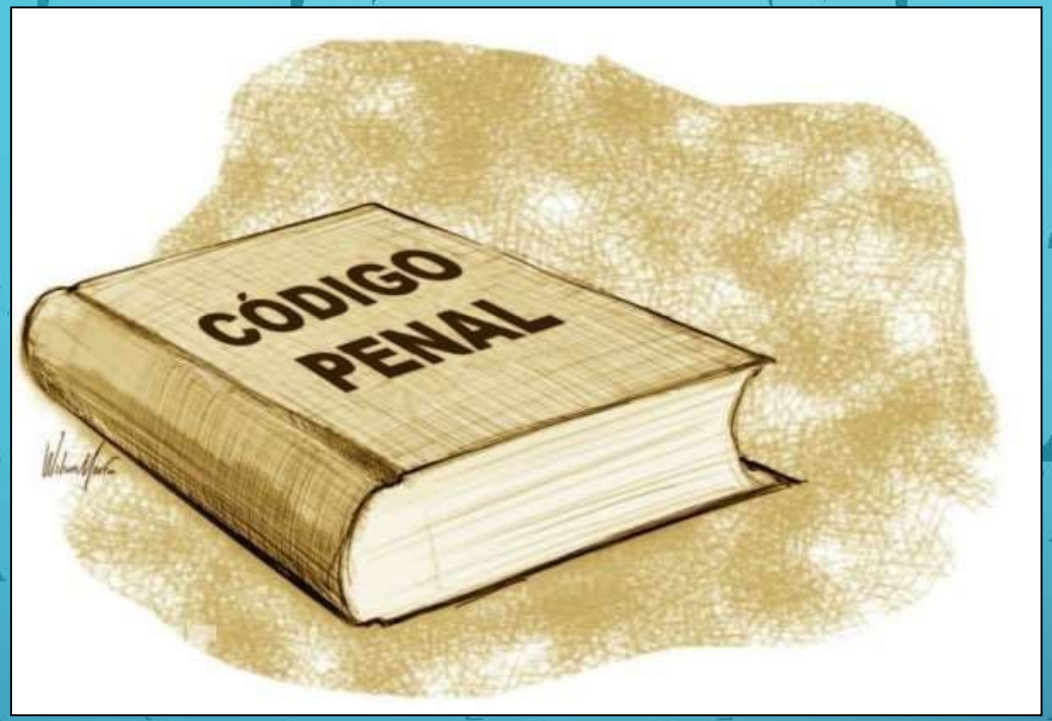
Rosalina Gonçalves da Cunha

Vanderlei Flores de Oliveira

ESTELIONATO ELETRÔNICO

INTRODUÇÃO

ERA DIGITAL – TECNOLOGIA – QUEBRANDO FRONTEIRAS



LEI 14.155 DE 2021 – ALTERAÇÃO SIGNIFICATIVA

COM A TIPIFICAÇÃO DE CRIMES DIGITAIS, AS FRAUDES POR MEIO DE TRANSAÇÕES DIGITAIS, POR EXEMPLO O PIX, AS COMPRAS ONLINE DE CARTÕES DE CRÉDITO, CLONAGEM DE APLICATIVOS COMO O WHATSAPP, SERÃO PUNIDAS.

ESTELIONATO X ESTELIONATO ELETRÔNICO

Estelionato

- Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
- Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Fraude Eletrônica

- Art. 171, § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A LGPD regulamenta a coleta, tratamento e armazenamento de dados pessoais no Brasil, assegurando direitos individuais.

Sua importância reside em proteger a privacidade dos cidadãos, promover a transparência nas operações digitais e alinhar o país com padrões internacionais de proteção de dados.

OBJETIVOS E CARACTERÍSTICAS

- Requer justificação legal para a manipulação de dados pessoais em contextos públicos e privados.
- Destaca o consentimento do titular como central para proteger direitos e liberdades individuais.
- Busca estabelecer um referencial legal para proteger a privacidade e direitos individuais na era tecnológica.
- Define bases legais, regulamenta o consentimento e promove informações seguras e responsáveis.
- Impulsiona uma cultura de responsabilidade, transparência e respeito às liberdades individuais em um mundo cada vez mais conectado.

O QUE É O PHISHING?

- O phishing é um tipo de fraude online, para obter informações confidenciais dos usuários.

EM QUE CONSISTE?

- Os criminosos falsificam a identidade de empresas ou instituições conhecidas e pelo engano, tentam que os utilizadores, facilitem informações.

COMO FAZEM?

- ATRAVÉS DE E-MAIL

- SMS, MENSAGENS INSTANTÂNEAS

COMO SE PROTEGER CONTRA O PHISHING?

- SEMPRE VERIFIQUE A DIREÇÃO DO E-MAIL SE CORRESPONDE A QUEM ENVIOU

- VERIFIQUE A AUTENTICIDADE DA PÁGINA QUE VOCÊ FORNECE SEUS DADOS!

GOLPES NO WHATSAPP

WhatsApp é um dos mais utilizados no mundo e consequentemente o que mais atrai os golpistas. Se aproveitando de momentos de distração do usuário, criminosos praticam roubos de senhas e dados pessoais para tirar alguma vantagem ilícita.

PRINCIPAIS GOLPES NO WHATSAPP

- Novo Número ou perfil falso (conseguir transferências de amigos da vítima);
- Auxílio Econômico falso (roubar dados pessoais);
- Clonagem do número de WhatsApp (conseguir dados pessoais e/ou conseguir transferências dos conhecidos da vítima);
- Aplicativos de Spyware (roubar dados pessoais);
- Golpe de notícias falsas (roubar dados pessoais);
- Golpe do falso emprego;
- Falsas atualizações do WhatsApp (instalar vírus ou spyware no celular e roubar dados pessoais).

COMO RELATAR GOLPES ÀS PLATAFORMAS DE REDES SOCIAIS?

PASSO 1: IDENTIFICAÇÃO DO GOLPE

- Observe mensagens suspeitas ou fraudulentas, como por exemplo aquelas costumeiras mensagens recebidas pelo SMS, pedindo para acessar um link, ou pedindo para dar a confirmação de um código, etc;
- Sempre desconfie se alguém solicitar informações pessoais, como por exemplo informações bancárias, dados de cartões, código de segurança do cartão, senha de aplicativos, etc.
- Consulte se o CNPJ da loja consta no site da Receita Federal, bem como se a loja consta na lista do Procon. Verifique aindase a loja protege seus dados e se possui certificado SSL e fique atento ao endereço (URL) de sites.

PASSO 2: CAPTURA DE EVIDÊNCIAS

- Tire screenshots dessas interações suspeitas, perfis envolvidos ou qualquer evidência relacionada ao golpe. Essas evidências servirão de provas para relatar a situação e serão essenciais.

PASSO 3: RELATÓRIO À PLATAFORMA DE REDE SOCIAL

- Acesse as configurações de ajuda ou suporte da plataforma e siga os procedimentos para denunciar o perfil ou postagem fraudulenta.
- Quando um post é reportado, as empresas analisam e firmam uma decisão de acordo com a política da plataforma,evitando fraudes e estelionatos, entre outros conteúdos inadequados.

FACEBOOK:

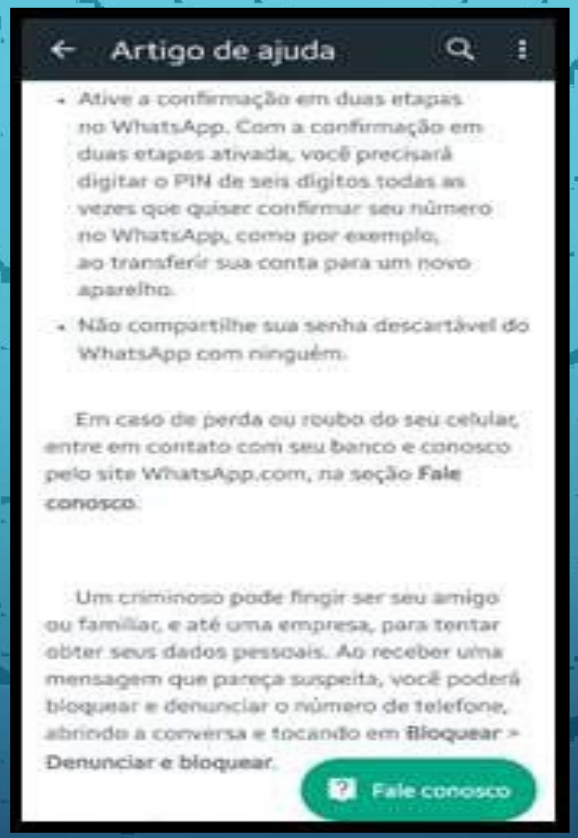

Central de Ajuda
Como denunciar algo
Denunciar um conteúdo impróprio ou abusivo no Facebook (por exemplo, nudez, discurso de ódio ou ameaças)
O que fazer se alguém estiver incomodando você por mensagens no Facebook
Como faço para denunciar algo no Facebook se não tenho uma conta ou não consigo ver o conteúdo?
Como denunciar uma conta ou Página do Facebook que está fingindo ser eu ou outra pessoa
Perfis e Páginas que se passam por outras pessoas violam os Padrões da Comunidade e são proibidos no Facebook.
Caso veja um perfil ou uma Página que esteja fingindo ser você, alguém que conheça ou uma figura pública (por exemplo, uma celebridade ou um político), entre em contato conosco. É possível denunciar perfis ou Páginas que se passam por outras pessoas mesmo se você não tenha uma conta do Facebook.


Central de Ajuda
Experiência clássica do navegador para celular
Denunciar um perfil
Se você tem uma conta do Facebook e deseja denunciar um perfil:
1 Acesse o perfil impostor.
• Caso não consiga encontrá-lo, tente pesquisar o nome usado no perfil ou perguntar a amigos se eles podem enviar um link para você.
2 Toque em sob a foto da capa e selecione Obter apoio ou denunciar perfil.
3 Siga as instruções na tela para enviar a denúncia sobre imitação de identidade.


Central de Ajuda
Denunciar uma Página
1 Abra o aplicativo do Facebook para iOS ou Android.
2 Acesse a Página falsa.
3 Toque em no canto superior direito e selecione Obter apoio ou denunciar Página.
4 Selecione Golpes e Páginas falsas.
5 Selecione a opção que melhor descreve a Página impostora.
6 Toque em Avançar.
Denunciar sem uma conta
Se você não tem uma conta do Facebook ou perdeu o acesso à sua, ainda pode denunciar uma Página ou conta impostora.
• Preencha o formulário de contato para denunciar uma Página ou conta impostora.
Você também pode denunciar Páginas ou perfis impostores no Messenger. Saiba como na Central de Ajuda do Messenger.

WHATSAPP:


Artigo de ajuda
Dicas para evitar fraudes ao usar o serviço de pagamentos no WhatsApp
Você pode ajudar a manter suas informações seguras para que nenhuma outra pessoa tenha acesso a elas, mesmo em caso de perda ou roubo do seu celular. Confira algumas dicas:
• Ative o bloqueio por impressão digital, Touch ID ou Face ID no seu aparelho. Após configurar essa opção, você precisará desbloquear seu app toda vez que abri-lo.
• Defina uma senha segura para a tela de bloqueio do seu aparelho. Evite senhas fáceis de adivinhar, como datas de aniversário, endereços, números de telefone, combinações numéricas simples, nomes de animais de estimação etc.


Artigo de ajuda
• Ative a confirmação em duas etapas no WhatsApp. Com a confirmação em duas etapas ativada, você precisará digitar o PIN de seis dígitos todas as vezes que quiser confirmar seu número no WhatsApp, como por exemplo, ao transferir sua conta para um novo aparelho.
• Não compartilhe sua senha descartável do WhatsApp com ninguém.
Em caso de perda ou roubo do seu celular, entre em contato com seu banco e conosco pelo site WhatsApp.com, na seção Fale conosco.
Um criminoso pode fingir ser seu amigo ou familiar, e até uma empresa, para tentar obter seus dados pessoais. Ao receber uma mensagem que pareça suspeita, você poderá bloquear e denunciar o número de telefone, abrindo a conversa e tocando em Bloquear > Denunciar e bloquear.
Fale conosco


Artigo de ajuda
• Ative a confirmação em duas etapas no WhatsApp. Com a confirmação em duas etapas ativada, você precisará digitar o PIN de seis dígitos todas as vezes que quiser confirmar seu número no WhatsApp, como por exemplo, ao transferir sua conta para um novo aparelho.
• Não compartilhe sua senha descartável do WhatsApp com ninguém.
Em caso de perda ou roubo do seu celular, entre em contato com seu banco e conosco pelo site WhatsApp.com, na seção Fale conosco.
Um criminoso pode fingir ser seu amigo ou familiar, e até uma empresa, para tentar obter seus dados pessoais. Ao receber uma mensagem que pareça suspeita, você poderá bloquear e denunciar o número de telefone, abrindo a conversa e tocando em Bloquear > Denunciar e bloquear.
Fale conosco

PASSO 4: COMPARTILHE COM SUA REDE

- Alerte amigos e familiares sobre esse golpe, evitando que mais pessoas caiam nessa armadilha. Lembre-se, quanto mais o compartilhamento e a informação acerca de um golpe, mais protegidas e menos propensas a se tornarem vítimas estarão, especialmente os mais vulneráveis, como os idosos e as crianças, explicando como vem acontecendo esses golpes de estelionato eletrônico e ensiná-los a se protegerem.

PASSO 5: DENÚNCIA ÀS AUTORIDADES COMPETENTES

- Se o golpe envolver atividades criminosas, como roubo de dados pessoais ou fraudes financeiras, denuncie à Polícia Civil ou ao Ministério Público.
- Faça um Boletim de Ocorrência, levando as evidências a uma delegacia para formalizar a denúncia do caso, fazendo com que sejam investigadas.
- Para verificar a existência de uma delegacia personalizada, recomenda-se acessar o site Safernet, possibilitando consultar a localização e acesso a informações atualizadas com enfoque em crimes virtuais.
- Acesse por QR CODE direcionando a câmera de celular para o código ao lado:

CONSIDERAÇÕES FINAIS

- O CRIME SE ADEQUOU AS TECNOLOGIAS DIGITAIS;
- FACILIDADE E ACESSIBILIDADE
- RELEVÂNCIA SOCIAL

DENUNCIE E

COMPARTILHE!

A luta contra o estelionato eletrônico não é apenas responsabilidade individual; é uma ação coletiva. Compartilhar informações sobre golpes e denunciá-los é crucial para proteger nossa comunidade digital.

INSTRUÇÕES PARA DENUNCIAR:

- **Reúna Evidências:** Capture informações e utilize os recursos de denúncia das redes sociais ou sites envolvidos.
- **Denuncie às Autoridades:** Em caso de atividades criminosas, denuncie à Polícia Civil ou Ministério Público, entregando todas as evidências disponíveis, e alerte amigos e familiares para promover a segurança digital.

UNI PROCESSUS centro universitário

LGPD

UNIDOS CONTRA O ESTELIONATO ELETRÔNICO!

Estamos todos conectados nesta era digital e, juntos, somos mais fortes. A ação coletiva é a chave para um ambiente online seguro. Ao compartilhar conhecimento, denunciar golpes e proteger uns aos outros, estamos construindo um mundo digital mais seguro e resistente ao estelionato eletrônico.

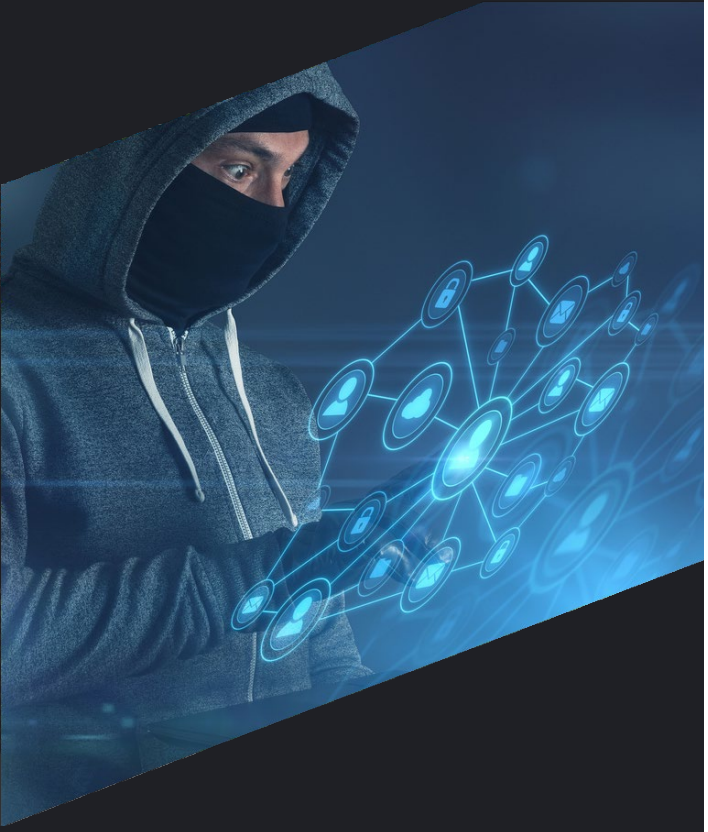
Junte-se à causa, seja parte da solução e inspire outros a fazerem o mesmo. Unidos, podemos vencer essa batalha contra as ameaças cibernéticas.

ATIVIDADE REALIZADA PELOS ALUNOS DA DISCIPLINA EXTENSIONISTA "DIREITO DIGITAL", TURNO NOTURNO, CAMPUS DA ASA SUL:

Caroline Batistella
Erivelto Drumond Ponte
Gabrielly Ogawa de Abreu
Iris Portela Gomiero
João Pedro Mendes de Souza
Kallel Filipe dos Santos Araújo
Marcello Carvalho de Araújo
Rosalina Gonçalves da Cunha
Vanderlei Flores de Oliveira

ESTELIONATO ELETRÔNICO: O INIMIGO DIGITAL

Proteja-se agora contra os golpes cibernéticos!



O QUE É

ESTELIONATO ELETRÔNICO?

Na era digital, onde a tecnologia nos conecta e simplifica nossas vidas, também enfrentamos o crescente perigo do estelionato eletrônico. Este inimigo oculto aproveita-se das vantagens da era digital para nos ameaçar.

Neste folheto, desvendaremos os riscos e aprenderemos a proteger-nos dessas ameaças.

CONHEÇA OS GOLPES CIBERNÉTICOS

No vasto mundo digital, espreitam armadilhas traiçoeiras que podem prejudicar nossas vidas online e até mesmo a segurança pessoal. **Esteja atento às seguintes ameaças:**

PHISHING:

E- mails e mensagens falsas que buscam enganar e obter informações confidenciais.

CLONAGEM DE WHATSAPP:

Golpistas que se fazem passar por amigos próximos para solicitar ajuda financeira ou informações pessoais.

FALSAS ATUALIZAÇÕES:

Promessas de atualizações tentadoras que, na verdade, escondem vírus e malware.

MANTENHA-SE

SEGURO ONLINE

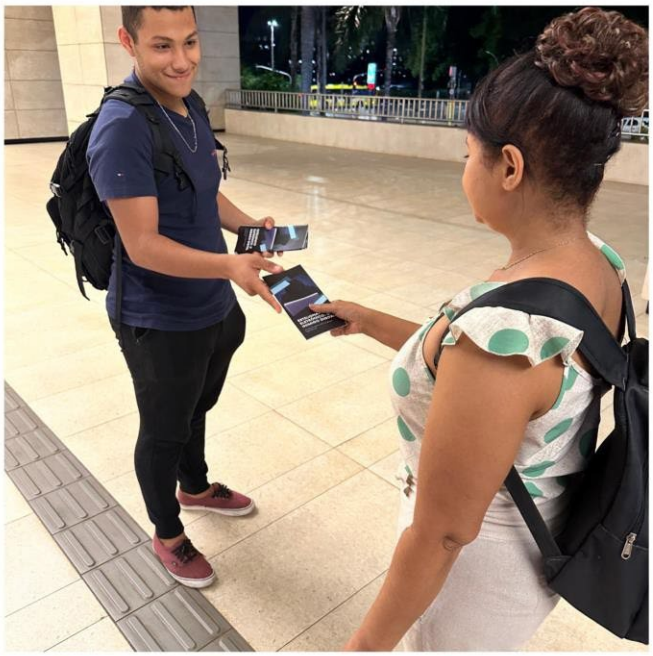
Para defender-se das ameaças digitais, adote medidas de segurança sólidas, incluindo:

1. **Autenticação de Dois Fatores (2FA):** Ative 2FA sempre que possível para uma camada extra de segurança.
2. **Senhas Robustas:** Crie senhas complexas e únicas para cada conta, utilizando letras, números e caracteres especiais.
3. **Educação Digital:** Mantenha-se informado sobre as táticas dos golpistas e esteja atento a links e mensagens suspeitas.

Execução: Entrega das cartilhas.


RAMONES


CONSTANCE




RAMONES


RIACHUELO