INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES MUNICIPAIS – IPSEMC
CNPJ Nº 41.216.755/0001-05



CARTILHA BÁSICA DE SEGURANÇA DIGITAL: para aposentados e pensionistas do Ipsemc V. 01

PROGRAMA DE EDUCAÇÃO PREVIDENCIÁRIA - PEP

CABEDELO-PB
2017

"A única segurança verdadeira consiste numa reserva de sabedoria, de experiência e de competência."
(Henry Ford)

INTRODUÇÃO

Este projeto de disponibilizar uma cartilha básica de segurança digital nasceu pela necessidade de enfrentar a avalanche de notícias e publicações veiculadas na mídia e nas redes sociais sobre fraudes realizadas no meio digital, das quais, conforme informações divulgadas no Estadão, Comitê Gestor da Internet no Brasil - CGI, Polícia Federal, entre outros, os idosos representam o grupo que mais são vítimas de golpes, ou seja, são os mais fácil e frequentemente enganados na internet.

Outro fator que levou à criação dessa cartilha foi o medo de sofrer golpes e as dificuldades de identificá-los na internet, fatos relatados em diálogos informais pelos próprios aposentados vinculados ao instituto, cuja faixa etária, em boa parte, está acima dos 60. Por exemplo, "recebo um e-mail do Banco do Brasil, com logotipo do Banco do Brasil, dirigido à minha pessoa e eu realmente tenho uma conta no Banco do Brasil, mas o e-mail solicita meus dados pessoais e tudo pode ser resolvido clicando em um link destacado na mensagem. Desconfiar ou Confiar? Mas o que pode acontecer com um simples clique?".

Outro problema identificado no comportamento digital dos aposentados e ainda nos alunos do grupo de atividades integrativas - programa desenvolvido pelo Ipsemc em parceria com o Centro de Convivência do Idoso (CCI), que promove qualidade de vida às pessoas da Terceira Idade – é a facilidade com que compartilham notícias falsas (*fake news*) e boatos. Geralmente, tais (des)informações são feitas de uma maneira convincente, mas com dados muitas vezes sem fundamento e com fontes ou erradamente indicadas ou sem nenhuma credibilidade, só que tais boatos e notícias falsas chegam nos celulares e notebooks e automaticamente as pessoas repassam nas redes sociais e comunicadores instantâneos sem o menor questionamento, muitas vezes pensando estar fazendo algo bom.

Então, essas e várias outras dúvidas e situações novas incorporadas ao meio digital de diferentes formas pode confundir a cabeça dos usuários, principalmente enquanto não houver uma maior conscientização sobre as fraudes realizadas por meio da internet e ainda facilitadas pela falta de entendimento sobre segurança de notebooks, smartphones

e dispositivos semelhantes. Bem como pela falta de orientações sobre como identificar um boato ou notícia falsa.

Jackson Angelo Pereira
Chefe do Setor de Processamento de Dados

1. APRESENTAÇÃO

É preciso entender que neste instante, a faixa etária da Terceira Idade certamente ainda não tinha acesso à internet e dispositivos tão avançados em idades anteriores (infância, adolescência, juventude), visto que o *boom* dos dispositivos como *notebooks* e *smartphone*s só se iniciou nos anos 90 e se intensificou a partir do início do novo milênio, sendo que a internet mesmo e as redes sociais demoraram um pouco mais para serem utilizadas pelas classes mais pobres. Isso sem falar ainda nas pessoas que viviam e ainda vivem em regiões muito isoladas e sem acesso às tecnologias digitais.

Por outra lado, é preciso reconhecer também o quão maravilhosos sãos os recursos e possibilidades advindos com o mundo digital, principalmente para quem foi de uma época em que eles não existiam: comunicação instantânea com pessoas e familiares de qualquer lugar do mundo, ter acesso e acompanhar informações e notícias em tempo real, uma gama sem fim de conhecimentos, acesso a músicas, vídeos e livros em formato digital e carregá-los num dispositivo que cabe em suas mãos, entre múltiplas possibilidades.

É inegável que o meio virtual pode trazer consideráveis benefícios para a saúde física e mental dos idosos, como melhorar a memória e a concentração por meio de jogos e aplicativos diversos, podendo deixar ainda sua mente suficientemente ocupada. A internet também permite uma melhor interação e integração com os grupos e pessoas com quem se identificam, o que ajuda a manter e fortificar os laços afetivos. Só que a maior parte dessas ferramentas lúdicas, comunicacionais e interativas exigem o fornecimento de dados pessoais, que constituem a razão da "corrida pelo ouro" de pessoas ou grupos fraudulentos ávidas em roubar, se apossar desses dados para cometer diversos tipos de crimes, principalmente financeiros.

Mas, ao lado de todas essas maravilhas do mundo digital da atualidade, temos também muitos problemas, armadilhas e pessoas mal-intencionadas a fim de roubar dados privados de pessoas e organizações, e, no fato que mais nos interessa aqui, aplicar golpes, especialmente financeiros, em suas vítimas. E ao mesmo tempo em que o usuário pode se comunicar com sua família do outro lado do mundo em tempo real, outra pessoa de algum outro lugar do mundo sem ser percebida pode estar acessando sua máquina e roubando dados conforme seus interesses.

A desinformação, a possibilidade de veicular calúnias, injúrias e difamações no meio digital e ainda boatos e compartilhar "fatos" e "pessoas" que nunca existiram também é muito grande. Artistas, políticos, altos líderes religiosos, pessoas influentes e famosas de todo o mundo certamente já foram vítimas de algum boato. E a principal forma desses boatos e desinformações serem passados adiante é os celulares e computadores dos cidadãos comuns que ingenuamente e sem conhecer a dimensão prejudicial desta prática de clique em clique compartilham em nível exponencial tais mensagens.

Feitas estas considerações, não é difícil entender que cada pessoa que possui um celular, que utiliza Whatsapp, Messenger e programas afins, bem como Instagram Facebook, Twitter deve estar atento ao que compartilha, principalmente porque há legislação específica aplicável a tais práticas e nenhum de nós quer ser responsabilizado criminalmente por compartilhar uma informação falsa.

Devemos ainda estar atentos e conhecermos os principais meios pelos quais as fraudes ocorrem na internet. E o Ipsemc, bem como todo RPPS, deve estar consciente desta realidade, a fim de que seus usuários, beneficiários ou mesmo sua equipe não caiam em golpes que podem até utilizar e prejudicar tanto o nome quanto as finanças da instituição.

Esperamos que esta cartilha básica, a qual se completa com uma série de reuniões e diálogos que teremos com nossos beneficiários e alunos das atividades integrativas com essa temática, possa cumprir seus objetivos ajudando a minimizar a possibilidade de fraudes e o compartilhamento irresponsável - ou, por que não dizer ingênuo? - identificados de forma geral na sociedade e, de modo especial, para nós, no grupo de nossos beneficiários e alunos do programa de atividades integrativas.

Certificação Profissional ANBIMA CPA-10

Léa Santana Praxedes
Presidente
lea@ipsemc.pb.gov.br
83 3228.4799 / 1434

2. JUSTIFICATIVA

O Instituto de Previdência dos Servidores Municipais de Cabedelo – IPSEMC compreende a necessidade de se adequar às novas exigências da atualidade e ajustar os seus procedimentos, principalmente no que diz respeito à sensibilização e preparação dos seus servidores, bem como aposentados e pensionistas para a vida moderna, na qual vivemos um momento de perplexidade e mudanças em várias esferas, sendo que o meio digital tornou-se parte de nossas vidas, de tal forma que tudo passa por ela:

- Comunicação fácil com outras pessoas, instituições, grupos etc.;
- Compras, trocas e diversas formas de negócios online;
- E-mails de pessoas e instituições que conhecemos e de quem nunca ouvimos falar;
- Notícias em tempo real;
- Boatos e desinformação em tempo real;
- Crimes, fraudes, golpes, violência, *bullying*, agressão online por meio de um simples clique;
- Acervo de filmes, músicas, vídeos, livros, jogos, diversões online de todo tipo;
- Compartilhamento de informações pessoais extremamente facilitado mas, ao mesmo tempo perigoso, como a localização pessoal disponível em celulares e até mesmo em programas de computador;
- Transações com cartão de crédito;
- Compra de ingressos para todo tipo de evento;
- Compras de passagens de avião, ônibus etc.;
- Reservas em hotéis, clubes e todo tipo de casa para acomodação temporária de pessoas;
- Estudos e cursos online, com aulas online, material online etc.

É UM "MUNDONLINE". Tudo está na linha do meio digital.

Assim, é preciso tanto saber aproveitar as possibilidades de interação e de saciação de nossas necessidades e desejos quanto saber fazer isso de forma segura, sem que haja prejuízos para nós nem para terceiros.

Estar informado sempre foi uma necessidade da vida humana e é verdade que há pessoas e veículos de comunicação que cumprem com dignidade, submissos à verdade, ao profissionalismo e aos princípios éticos este papel. Mas, atualmente, muitas pessoas e grupos mal-intencionadas se aproveitam da exponencial facilidade de compartilhamento de informações e criam mentiras, calúnias, injúrias, difamações e boatos a fim de prejudicar a imagem e conceito de outra pessoa ou uma instituição.

O costume de acreditar em tudo que se lê aliado ao fato das pessoas que absorvem tais informações não checarem as respectivas fontes de publicação torna o ambiente ainda mais propício para seu compartilhamento, que, dependendo do objetivo, tanto pode ferir, machucar, denegrir a pessoas e instituições inocentes.

Tais fatos, corroborados pelo fato de que as pessoas da Terceira Idade ainda são as que mais sofrem com a prática de fraudes online, nos faz acreditar que essa cartilha básica pode ajudá-las a ter mais confiança e segurança no uso de internet e dos meios que esta possibilita para interação com o mundo e com as pessoas e administração sensata de seus dados pessoais.

3. OBJETIVOS

Ensinar e garantir uma prática mais segura de internet junto aos aposentados e alunos do programa de atividades integrativas do Ipsemc, os quais, em sua maioria, fazem parte do grupo de Terceira Idade.

4. OBJETIVOS ESPECÍFICOS

a) Despertar uma consciência junto ao público-alvo da cartilha de que é preciso tomar cuidados diversos na administração de dados pessoais na internet (senhas, e-mails, nome completo, número de documentos e contas bancárias etc.);

b) Garantir ao público-alvo o conhecimento básico das informações referentes à segurança na internet (golpes e boatos/desinformação), bem como evitar/minimizar riscos de incidência destas situações;

c) Esclarecer os principais tipos de fraudes e como evitar cair nelas;

d) Esclarecer as principais características de um boato e ajudar a identifica-los.

]

5. PÚBLICO-ALVO

Aposentados e pensionistas do Ipsemc, grupo do programa de atividades integrativas do Ipsemc, bem como pessoas da Terceira idade em geral, pela sua aplicabilidade.

6. SISTEMÁTICA

No que diz respeito aos passos a serem dados pelo Programa de Educação Previdenciária – PEP e de Preparação para Aposentadoria – PPA, aqui consubstanciado na Cartilha Básica de Segurança na Internet, será desenvolvido, a princípio, da seguinte forma:

a) Elaboração da cartilha básica de segurança na internet;
b) Realização de eventos de conscientização do tema junto ao principal público-alvo;
c) Tira-dúvidas individualizado para integrantes do principal público-alvo sobre a temática, sempre que solicitado.
d) Distribuição da cartilha em meio online ou físico, bem como material de outras instituições que possam enriquecer e facilitar o conhecimento da temática.

O eventos e realizações serão divididos em duas partes: na primeira, o público-alvo principal receberá material informativo a fim de assimilar os conceitos e poderá fazer perguntas, questionamentos e tirar suas dúvidas. Na segunda parte, de caráter prático, os participantes experimentarão situações que simulam ações de golpes online e identificação de boatos e notícias falsas.

Na metodologia empregada poderão ser aplicadas ainda técnicas de dinâmica de grupo para melhor entendimento da temática.

7. FRAUDES: CONCEITOS E PRINCIPAIS TIPOS

7.1 CONTEXTO

De acordo com recente levantamento do Comitê Gestor da Internet (CGI), há dez anos atrás, 4% dos idosos no País acessavam a rede, número que cresceu para 20%, tornando sua participação nas redes sociais muito maior. Por exemplo, perfis de brasileiros acima de 60 anos que utilizam o Facebook passa dos 4 milhões de usuários nos dias atuais.

A Kaspersky, empresa mundialmente líder em programas de segurança, afirma que, conforme suas pesquisas, os idosos são os que mais são vítimas de fraudes e que os golpistas ajustam suas práticas criminosas ao saber se tratar de pessoas desta faixa etária. O idosos por não ter muito conhecimento de segurança ou fraudes na web ainda não sabe diferenciar a fraude de algo legítimo.

7.2 CONCEITOS E EXEMPLOS

A fraude, no sentido que vamos tomar nesta cartilha básica, em Direito Penal, é o crime ou ofensa de deliberadamente enganar outros com o propósito de prejudicá-los, usualmente para obter propriedade ou serviços dele ou dela injustamente. Trata-se de um ato ilícito ou de má-fé feito com o objetivo de obter vantagens indevidas de terceiros, sempre se utilizando de meios para omitir informações, enganar, mentir, quebrar normas, inverdades intencionais etc.

Alguns exemplos de fraudes:

- Propaganda enganosa
- Roubo ou criação de "identidades falsas" (pessoas e empresas);
- Esquema em pirâmide
- Falsificação de documentos ou assinaturas
- Apropriação de propriedade de outros sob custódia através da violação de confiança
- Fraude da saúde, vendendo produtos inócuos, como remédios falsos
- Criação de empresas falsas
- Insolvência de instituições bancárias e de seguro
- Falsificação de documentos em geral
- Falsificação de assinaturas documentos, ordens de pagamento, cheques etc.
- Simulação de situações e fatos

7.3 FRAUDES MAIS COMUNS NA INTERNET CONTRA PESSOAS DA TERCEIRA IDADE

No Brasil, conforme divulgado em diferentes pesquisa e ainda de acordo com informações do CGI, PF, Globo Online e diversos veículos de comunicação, entre as fraudes mais comuns praticadas por meio da internet contra os idosos podem ser citados os seguintes:

Processo Jurídico - geralmente um escritório de advocacia desconhecido envia carta ou e-mail ao aposentado alegando que existe por meio jurídico uma forma de corrigir e aumentar em, digamos, 40%, 50% o valor da aposentadoria, ou ainda que existem valores atrasados ou bloqueados. No e-mail pode ser exigido o acesso a algum site para preenchimento e envio de dados pessoais do aposentado: nome completo da pessoa, do pai e da mãe, data de nascimento, número de CPF, PIS, RG, endereço, dados bancários e do cartão de recebimento, entre outros. Em alguns casos, podem não exigir dados pessoais, mas solicitam uma quantia em dinheiro para que deem início ao processo de aumento garantido. O golpista se utiliza de termos comuns da área jurídica e transmite até algum conhecimento do assunto. Mas, trata-se de um golpe.

Empréstimo consignado - corresponde a 80% dos golpes praticados contra os idosos. Na internet, também são oferecidos empréstimos via e-mail ou Whatsapp, Messenger, redes sociais, entre outros. O idoso é uma vítima importante deste tipo de fraude em virtude das facilidades que eles têm de contrair empréstimo. No caso de receber e-mail ou mensagens em alguma plataforma digital com uma tentadora oferta de empréstimo consignado para aposentados e pensionistas, desconfie e não vá m frente. Principalmente, se o e-mail indicar um link para concessão do empréstimo e for direcionado a um processo eletrônico que exige o preenchimento de dados pessoais ou envio de cópias de seus documentos pessoais.

Se o e-mail, no caso aqui enfocado, tiver logotipo de Banco do Brasil, Caixa Econômica, Santander, Bradesco, entre outros bancos bem conhecidos, então descarte mesmo o e-mail e considere-o como golpe. Tais instituições não irão contatar o aposentado ou pensionista desta forma e por meio de e-mail, ainda mais se neste e-mail o destinatário for tratado apenas de senhor, pois seria normal inserir o nome completo da pessoa. Outro indício de ser golpe é a linguagem bagunçada, com erros de português. Os

endereços eletrônicos acessados muito diferentes dos verdadeiros também são indícios de um site fraudulento.

No caso do Ipsemc, o processo do empréstimo consignado é feito apenas presencialmente, no horário das 8h às 14h, na sede do instituto, pelo próprio beneficiário, munido dos seus documentos pessoais ou por meio de representante juridicamente definido em procuração registrada em Cartório. No ato, o beneficiário ou legítimo representante receberá um documento com seus dados e a margem (maior valor possível para desconto mensal) de empréstimo consignável para se dirigir à instituição bancária.

IMPORTANTE: embora não existam caso registrados de golpes envolvendo recadastramento de RPPS, mas já pensando em logo informar contra esta possibilidade, é oportuno reafirmar que o censo previdenciário do Ipsemc é realizado anualmente. O beneficiário (aposentado, pensionista) do Ipsemc deve, no mês do seu aniversário, dirigir-se pessoalmente ou por meio de representante legal à sede do instituto, no horário das 8h às 14h, munido de documentação pessoal a fim de atualizar seus dados cadastrais. O Ipsemc não oferece nenhum outro meio para isso. O Ipsemc pode até contatar por celular o beneficiário, mas o processo de recadastro é sempre realizado no prédio do instituto, A não ser em casos excepcionais definidos na Portaria do Censo.

Falsos e-mails de instituições financeiras - parecido com o golpe do empréstimo consignável via internet, só que, geralmente, neste caso, o indivíduo recebe e-mails que apontam a necessidade de atualização de dados cadastrais junto a alguma instituição financeira. Por sua vez, os bancos só informam necessidade de atualização de dados por telefone ou, em alguns casos, representantes se dirigem pessoalmente à residência do indivíduo que possua contas e contratos na agência. Mas, o processo de atualização de dados é sempre na agência. Neste caso, remova de sua caixa postal todo e-mail deste tipo e marque-o como spam (mensagem falsa), evitando que e-mails deste tipo continuem a aparecer em sua caixa postal.

Furto ou falsificação de identidade - ocorre quando uma pessoa tenta se passar por outra a fim de realizar atos ilícitos em nome dela. Há três possibilidades:

Primeira, alguém tenta se passar por outra pessoa que existe ou pode até nem existir a fim de enganar outro, adicionando a pessoa em uma rede social, solicitando número de celular ou Whatsapp, muitas vezes ganhando intimidade, marcando um encontro. É preciso entender que, neste caso, é alguém que você, por exemplo, não

conhece, então não confie em estranhos. Nem forneça detalhes sobre sua vida pessoal ou mesmo emocional assim tão ingenuamente. Se a pessoa insistir em pedir Whatsapp, por exemplo, faça uma ligação de vídeo, se a pessoa sempre se recusar ou encontrar alguma desculpa para não atender, então certamente é um perfil falso.

Segunda, a identidade utilizada pode ser de alguém que você realmente conhece. Esteja atento ao fato dela, por exemplo, adicionar você com um novo perfil no Facebook ou outra rede social sem eliminar o perfil já conhecido. Ligue, se tiver um número ou meio que você já possua de contato, ou tente falar com a pessoa que você conhece e certifique-se de que aquele perfil é dela ou não. Caso não seja, exclua a pessoa ou bloqueie.

Terceira, a identidade roubada pode ser a sua própria. Em termos de internet, por algum meio, alguém teve acesso ou roubou seus dados pessoais, como senha e nome de usuário de e-mail ou redes sociais, isto é, "raqueou", se apossou ilegalmente do seu perfil e passou a utilizá-lo para agir em seu nome. A pessoa então pode ter acesso a outros dados, como os de conta bancária e cartões caso haja anotado em e-mails e redes sociais; pode ver suas conversas. Neste caso, é importante sempre ter registrado em contas de e-mail e redes sociais um número de celular vinculado à conta e sempre atualizar, se mudar de número, este dado para conseguir com segurança recuperar sua conta. Vá à Delegacia de defraudações e falsificações, no bairro João Paulo II (Central de Polícia), telefone: (83) 3218-5333 e registre um boletim de ocorrência.

7.4 PRINCIPAIS CUIDADOS DE SEGURANÇA NA INTERNET A FIM DE EVITAR GOLPES

Peça ajuda aos seus parentes e escolha empresas de confiança – dê preferência, em caso de não ter muita segurança, e escolha pessoas de sua confiança a lhe ajudar com as questões de internet, sempre que tiver dúvidas. Em casos de compras e contratações online, busque por sites e empresas que já tenham nome solidificado e com credibilidade no mercado, por mais vantajosa que alguma oferta de um concorrente pareça.

Procure conhecer os controles de privacidade – toda rede social tem uma política de privacidade e configurações para o usuário limitar seu público e suas publicações. Se não souber, peça ajuda novamente a alguém de confiança. Só compartilhe fotos e informações de modo que sua vida privada, seu dia a dia não fique muito exposto. Evite

compartilhar onde se encontra, sua localização, inclusive no celular, a não ser com alguém do seu convívio e de sua confiança. Não aceite estranhos em redes sociais.

Não descuide do celular - muitas informações pessoais e aplicativos que dão acesso a contas bancárias e ainda vinculados a cartão de crédito, dados e mensagens pessoais, fotos íntimas podem estar armazenados no celular. Por isso, sempre tente deixar o celular com uma senha segura para travar a tela.

Desconfie de mensagens com promoções imperdíveis - por mais tentadoras que sejam, principalmente se não conhece o vendedor e se não tem experiência com compras online. Evite clicar nos links de compra que aparecem nestas mensagens que podem ser, na verdade, fraudulentos e conter vírus ou outras pragas virtuais.

Proteja-se contra vírus - tanto smartphones quanto computadores em geral precisam de antivírus para garantir a segurança dos mesmos. Existem antivírus pagos e gratuitos. Procure com uma pessoa de sua confiança informações a respeito, se não souber como escolher um. É sempre bom enfatizar que os antivírus e pragas virtuais afetam o desempenho da máquina e quase sempre o objetivo é roubar os dados pessoais do usuário para fins ilícitos. Uma vez escolhido um aplicativo de segurança, mantenha-o atualizado. O próprio programa vai exibir mensagens sobre necessidade de atualização.

E também é sempre recomendado manter todos os dispositivos instalados em sua máquina, seja computador ou celular, atualizados, porque nestes aplicativos são continuamente identificadas falhas principalmente de segurança, de uma ou outra forma encontrados por pessoas mal-intencionadas, que podem invadir o dispositivo.

Senha segura - utilize senhas seguras, a partir de 8 dígitos de preferência. Evite escolher datas de aniversários, seu nome ou de pessoas do seu convívio. Procure combinar letras maiúsculas e minúsculas, com números e símbolos também. Evite usar uma única senha para todos os serviços e dispositivos que utiliza. Se possível ou se não confiar totalmente em sua memória anote em um papel e mantenha a senha bem guardada. Não compartilhe a senha com outra pessoa.

Downloads - no caso dos celulares há dois principais aplicativos para baixar programas, são o Play Store para celular com sistema Android, que é a maioria, e Apple Store, exclusivo para Iphones. Só confie nestes canais. Fontes de terceiros não são recomendados e o próprio celular irá advertir em caso de instalação.

E-mails - se costuma usar e-mails, não confie em mensagens de contatos desconhecidos, ofertas irrecusáveis, comunicados de instituições bancárias, prêmios e sorteios (dos quais - você sequer lembra ter participado), comumente, são tentativas maliciosas de infectar o seu computador. Especialmente se tratando de e-mails com anexos e links. Nesses casos o recomendado é sempre atestar a confiabilidade da mensagem, confirmando sua procedência diretamente com o remetente.

Sair/Logout – se utilizar alguma senha de serviços que utiliza em algum computador ou celular que não seja o seu, sempre escolha a opção sair ou *logout* do aplicativo. Geralmente, é do lado esquerdo do aplicativo, mas pode estar bem escondido na opção perfil. Se tiver dificuldades, peça ajuda ao orientador da *wi-fi*, se for o caso, ou a alguém de sua confiança para sair do aplicativo, assim não estará ativo naquele dispositivo.

Há casos, porém, em que o e-mail parece ser até de alguém conhecido, mas o assunto e linguagem são diferentes do que você está acostumado a receber dela, e se é que ela já se comunicou por e-mail também. Desconfie se está noutro idioma, se apresenta ofertas de produtos a preços generosos, se pede para ver fotos acessíveis em um link suspeito. Procure saber com a pessoa se ela realmente mandou este e-mail. A regra é cautela sempre.

Com o tempo e a prática, estas recomendações já estarão incorporadas em sua forma de administrar seus dados pessoais em sua vida digital.

8. BOATOS E NOTÍCIAS FALSAS

8.1 CONTEXTO E CONCEITO

Este é um dos principais problemas virtuais da atualidade, porque além de golpes pode envolver questões como injúrias, calúnias, difamações, ofensa à moral de pessoas e instituições. Há casos registrados até de pessoas que foram assassinadas por conta de notícias ou informações falsas divulgadas sobre ela.

O boato é uma mensagem, não muito longa, que contém dados que podem ser totalmente falsos ou com partes verdadeiras (fatos) e partes falsas (inventadas, distorcidas). Pode vir ainda em forma de uma notícia, por exemplo, sobre uma figura pública, artista, político na qual se relata sua morte, problemas enfrentados, atos que ele tenha praticado ou sofrido, enfim, mas basicamente é constituído de algumas informações falsas, muitas vezes com intenção de prejudicar a imagem da pessoa retratada.

Antigamente era conhecido como hoax. Assuntos que despertam interesse como greves da Polícia Milita, greve dos bancos, cobrança de anuidade para quem tem carteira de habilitação, recebimento de PIS ou direitos trabalhistas para quem trabalhou em certo período do ano, algum tratamento maravilhoso e revolucionário também são temas de boatos.

Quem utiliza Facebook e Whatsapp ou dispositivos semelhantes certamente alguma vez já se deparou com um boato ou notícia falsa. Isso porque o usuário sem questionar sai compartilhando toda informação nova, surpreendente ou escandalosa que recebe. Mas o usuário tem que ter consciência de que só podemos sair repassando alguma informação baseado em fontes seguras.

É preciso estar ciente de que quem cria o boato assim como quem ajuda a espalhá-lo está sujeito a uma pena de 15 dias a seis meses de prisão ou pagamento de indenização, dependendo da gravidade do dano causado. Se causar danos e pânico por perigo irreal ou inexistente a um grupo ou população, o boato pode ser considerado uma contravenção penal referente à paz.

A lista de situações que envolvem boatos é extensa e pode ainda envolver ainda *cyberbullying* (*bullying* no meio digital), injúria, golpe financeiro. O boato ainda pode se

inserir em qualquer uma das três categorias existentes de crimes: aqueles de ação penal privada, em que apenas a própria vítima pode mover a ação; crimes de ação penal pública condicionados à representação, nos quais o Ministério Público (MP) pode mover processo após receber uma denúncia; e aqueles em que o próprio MP pode iniciar uma ação, quando se entende que o crime tem grande alcance e viola direitos básicos.

Quando o boato não fere ninguém muito menos gera danos, ele não é passível de pena, podendo ser interpretado como uma brincadeira pelo teor de sua mensagem.

Se a morte de alguém é ocasionada por conta de um boato compartilhado na internet, quem compartilhou pode estar sujeito a processo por incitação ao homicídio.

Conforme o site E-farsas (http://www.e-farsas.com, especializado em estudar e identificar boatos e notícias falsas), existem três características mais recorrentes dos boatos on-line: eles usam assuntos em voga (em moda, que chamam atenção na época) no momento; têm um tom conspiratório, pedindo para que as pessoas espalhem para o máximo de conhecidos; e em geral não são datados, o que permite que eles retornem de tempos em tempos.

Vejamos o título da chamada de alguns boatos:

"Vídeo comprova que o McDonald's serve alface artificial!"

"Escada cai em cima de crianças, mas elas saem ilesas!"

"A agência de publicidade de Sérgio Moro contratou a Madonna para vestir a camisa do PT"

"Criatura demoníaca é fotografada durante culto evangélico!"

"Projeto de Lei legaliza a Corrupção!"

"Sereia encontrada depois do Tsunami"

"Tubarão ataca helicóptero!"

Famosos que já tiveram morte anunciadas em boatos: Renato Aragão, Fernanda Montenegro, Reynaldo Gianecchini, Netinho, Ana Paula Arósio, entre muitos outros. Além do tema morte, são explorados falsamente temas como crimes, sequestros, ligações com grupos políticos, escândalos, amores e situações que nunca aconteceram.

Então, é preciso saber como identificar quando algo é realmente boato ou não antes de acreditar e sair compartilhando. A regra é: na dúvida não compartilhe.

8.2 COMO IDENTIFICAR UM BOATO

Busca em sites especializados: o meio mais rápido para saber se uma informação é boato ou não é realizando uma busca em sites especializados, os mais conhecidos são:

"Boatos": http://www.boatos.org/

"E-farsas": http://www.e-farsas.com/

Sobre temas relacionados a discursos políticos e pessoas da área política, podem ser consultados:

"Aos fatos": https://aosfatos.org/

"Lupa": http://piaui.folha.uol.com.br/lupa/

As seguintes informações foram retiradas do site "Catracalivre" (https://catracalivre.com.br) que compilou uma lista dos principais passos para verificar a autenticidade de uma informação e saber se uma mensagem é boato não:

1. Leia a mensagem completa - Mensagens falsas geralmente têm poucos detalhes, um texto vago e genérico, repleto de adjetivos e trechos em maiúsculas, que termina com um acontecimento trágico/dramático e muitos erros de português. Fique alerta! Quando a informação é frágil, é necessário usar de artifícios para dar uma inflada nela e fazer com que você acredite que ela é real.

2. Confira quando o tal fato ocorreu - Boatos não costumam ter a data de quando o pretenso fato aconteceu _ e, por isso, eles costumam ter vida longa, já que podem circular eternamente. Há também quem divulgue notícias reais, mas que aconteceram há anos e hoje não fazem mais sentido, como informações referentes a epidemias que não existem mais e decisões de governos antigos

3. Pesquise no Google - Sites como o Boatos.org, parceiro do Catraca Livre, e o E-Farsas fazem checagem de boatos de forma profissional. Discursos de políticos podem ser conferidos no Aos Fatos e na Agência Lupa. Além de conferir nestas plataformas, veja quais os sites que falam da tal notícia numa busca rápida no Google: se não houver nenhum site jornalístico confiável falando sobre o tema, evite compartilhar a informação.

4. Quem falou? - Quem é a fonte da mensagem? Boatos nem sempre citam quem é o autor da informação e, às vezes, mencionam alguma fonte conhecida, mas não incluem links que confirmem isso. Há também sites que disseminam informações falsas que clonam páginas de portais de notícias e têm um nome parecido com o destes portais. Parecidos,

mas não são os originais. Vá até os originais e cheque se a informação foi publicada realmente.

5. Veja se uma foto é real - Se você desconfiar da veracidade de alguma foto, procure observá-la bem e reconhecer se houve alguma alteração. Fique atento: a internet está repleta de montagens falsas. Além disso, o serviço de busca Google tem uma ferramenta que possibilita a localização de imagens com as mesmas características da foto baixada no seu computador ou de uma URL.

Repetindo, se houver dúvidas, mesmo tendo adotado todos estes passos, o ideal é não compartilhar. Se na verificação que fez identificou se tratar de um boato, avise a quem compartilhou sobre o boato ou insira em comentário um link para confirmar que a mensagem é falsa. Assim, evitará que o compartilhamento do boato continue e outras pessoas sejam erradamente informadas sobre algo que não existe ou não aconteceu, podendo evitar riscos a terceiros e até penalidades para quem compartilha boatos.