
TRT-11ª REGIÃO
Amazonas e Roraima
SEGURANÇA
PARA INTERNET

DIREÇÃO DO TRIBUNAL

Presidente
Desembargadora Ormy da Conceição Dias Bentes

Vice-Presidente
Desembargadora Solange Maria Santiago Morais

Corregedor Regional
Desembargadora Márcia Nunes da Silva Bessa

COMISSÃO DE SEGURANÇA PERMANENTE

Presidente
Desembargador Jorge Álvaro Marques Guedes

Membros
Juiz Audari Matos Lopes

Juiz Adelson Silva dos Santos

Juiza Gisele Araújo Loureiro de Lima

Ildefonso Rocha de Souza, Diretor-Geral

Ailton Luiz dos Santos, Chefe do Núcleo de Segurança Institucional

Sugestões para o aperfeiçoamento desta Cartilha poderão ser encaminhadas ao Núcleo de Segurança Institucional do Tribunal Regional do Trabalho da 11ª Região, ou pelo e-mail set.seguranca@trt11.jus.br.

EQUIPE DE ELABORAÇÃO E REVISÃO:

Chefe do Núcleo de Segurança Institucional
Maj QOPM Ailton Luiz dos Santos

Chefe da Seção de Gestão de Riscos de Segurança
CB QPPM Gutemberg Watson Gomes

Agente de Polícia Judicial
Ruy Fernando Ribeiro da Fonseca Júnior

COLABORAÇÃO:

Diretor da Secretaria de Tecnologia da Informação e Comunicações
Evandro Video de Souza Júnior

Chefe da Seção de Segurança da Informação
Jean Ricardo de Oliveira Rebouças

Agente de Polícia Judicial
Domingos Fabio dos Santos Coelho

Agente de Polícia Judicial
Francisco Cléber Coelho da Silva

DIAGRAMAÇÃO:

Seção de Gestão de Risco de Segurança

FOTOGRAFIA:

Seção de Gestão de Risco de Segurança

CAPA:

Seção de Gestão de Risco de Segurança

Sugestões para o aperfeiçoamento desta Cartilha poderão ser encaminhadas ao Núcleo de Segurança Institucional do Tribunal Regional do Trabalho da 11ª Região, ou pelo e-mail set.seguranca@trt11.jus.br.

SUMÁRIO

TRT-11ª REGIÃO
Amazonas e Roraima

ENGENHARIA SOCIAL

Técnicas de engenharia social estão sendo usadas para enganar usuários da internet e de aplicativos obtendo informações confidenciais sobre nome, senhas, detalhes do cartão de crédito ou clonagens. Para evitar esses transtornos vão aqui algumas dicas:

DICAS DE SEGURANÇA

❑ Oriente familiares, pessoas próximas e auxiliares da família sobre informações que são solicitadas na rua ou por telefone.

❑ Não clique em links desconhecidos em SMS, e-mails ou publicações em redes sociais.

❑ Não clique em banner de propagandas.

❑ Se houver perda de sinal da operadora e após o retorno do mesmo você começar a receber SMS ou qualquer outro tipo de mensagens de confirmação de reinstalação, sem que você tenha solicitado, desconfie.

❑ Se o seu celular foi perdido, furtado ou mesmo roubado, faça imediatamente um boletim de ocorrência e solicite o bloqueio de seu número de telefone junto a operadora.

❑ Tente sempre elaborar uma senha considerada forte, ou seja, difícil de ser descoberta, mas que você consiga se lembrar depois.

TRT-11ª REGIÃO
Amazonas e Roraima

PHISHING

Esse tipo de golpe tem o **objetivo de "pescar" informações e dados pessoais importantes, por meio de mensagens falsas.** Com isso, os criminosos podem conseguir nomes de usuários e senhas de um site qualquer, como também podem obter dados de contas bancárias e cartões de crédito.

As vítimas recebem link ou arquivo malicioso por e-mail, mensagem de texto (SMS) ou serviço de mensagem instantânea, como **WhatsApp**, **Telegram** e **Facebook** Messenger, que são criados para parecer emitidos por instituições conhecidas, como bancos, operadoras de telefonia, órgãos do Governo e administradoras de cartão de crédito. No ato de abrir o link ou arquivo, o celular ou computador é infectado por conteúdos fraudulentos que buscam dados pessoais e bancários.

Atualmente, são mais comumente propagadas as seguintes modalidades de **phishing**:

A) PHARMING: consiste no direcionamento da navegação do usuário para sites falsos;

B) SMISHINGS: são os **phishings** por SMS, enviados massivamente por meio de empresas especializadas em distribuição de mensagens em larga escala;

C) VISHING: é o **phishing** de chamada pela tecnologia VoIP (voz sobre IP), utilizado por criminosos para extrair dados bancários ou informações pessoais da vítima. São aplicadas técnicas de falseamento do remetente da chamada, possibilitando ao autor da chamada se passar por atendente bancário, de empresa comercial ou funcionário público;

D) "CHAT-IN-THE-MIDDLE": envolve a adição de uma janela de suporte de bate-papo ao vivo falsa, na qual a pessoa é estimulada a inserir seus nomes de usuário e senhas.

DICAS DE SEGURANÇA

❑ Lembre-se: phishing é um ataque oportunista. Não clique em links desconhecidos em mensagens de SMS, e-mails, WhatsApp ou publicações em redes sociais.

TRT-11ª REGIÃO
Amazonas e Roraima

BAITING

Nesse modelo de golpe, o criminoso "esquece" um pen drive em lugar de muita circulação, contando com a curiosidade do usuário para atraí-lo. Quando a vítima conecta o dispositivo no computador, é instalado um software malicioso sem que ela perceba.

CLONAGEM POR SIM SWAP

A técnica consiste em transferir a linha do chip de um usuário para um chip em branco. Esta modalidade pressupõe a participação de funcionários de empresas de telefonia ou de pessoas por estas autorizadas a realizar a migração de conta para outro usuário. Trata-se de operação ilegal, mas que vem se tornando corriqueira nos últimos anos. Esta situação é bastante delicada, pois as mensagens SMS dirigidas àquela conta passa a ter como destinatário o próprio criminoso. Desse modo, todos os aplicativos que possuem fator de segurança configurado para confirmação via códigos ou tokens encaminhados via SMS, tornam-se extremamente vulneráveis, como no caso de aplicativos bancários e o aplicativo Whatsapp. A conta deste aplicativo de mensageria facilmente é tomada pelo criminoso. Diferentemente dos demais casos, o usuário percebe que está completamente impedido de usar qualquer serviço da operadora, inclusive chamadas telefônicas.

COMO SE PROTEGER

❑ Inclua como fator de autenticação o cadastro de uma conta de e-mail válida e protegida por senha considerada forte. Para incluir esse dado na confirmação em duas etapas no WhatsApp, **abra: CONFIGURAÇÕES > CONTA > CONFIRMAÇÃO EM DUAS ETAPAS > ATIVAR.** Após definir a senha de 6 (seis) dígit os numéricos, incluir a conta de e-mail. Jamais enviar para outra pessoa a senha desta conta cadastrada.

VERIFICAÇÃO EM DUAS ETAPAS

A verificação em duas etapas ou autenticação de dois fatores é uma técnica de proteção utilizada por diversos sites e aplicações da web. A autenticação de senhas em duas etapas pode até não ser a solução definitiva para a segurança de contas, mas reduz o risco de que contas on-line, redes sociais e serviços bancários sejam atacados por hackers. Funciona, basicamente, como uma etapa a mais nos processos de autenticação de login e senha, que devem ser realizados pelo usuário.

TRT-11ª REGIÃO
Amazonas e Roraima

WHATSAPP

PREVENÇÃO: COMO EVITAR UM POSSÍVEL GOLPE

❑ Abra o aplicativo e vá **no canto superior direito do aplicativo (toque nos três pontinhos) > Configurações (android) / Ajustes (iOS) > Conta > Confirmação em duas etapas > Escolha 06 números (pin) > confirmação do pin > escolha um e-mail e ATIVAR.**

COMBATE E RECUPERAÇÃO: COMO AGIR APÓS UM GOLPE

❑ Informe através de outras redes sociais, ao maior número de pessoas possíveis acerca do ocorrido, para que eles não caiam no mesmo golpe e possam avisar outros amigos também.

❑ Enviar email para support@whatsapp.com, com o assunto: Whatsapp Clonado. Informe no corpo do email o número de telefone com o código do país e DDD da região. Ex: (+55 92 9XXXX-XXXX) e a descrição do ocorrido, também solicitando desativação da conta clonada.

❑ Com a desativação realizada, reinstale o aplicativo no seu celular e ative novamente sua conta.

TRT-11ª REGIÃO
Amazonas e Roraima

WHATSAPP

FOTOS DO PERFIL CLONADOS

Os criminosos vinculam a fotografia da vítima, normalmente retirada do próprio **WhatsApp** ou das redes sociais, a um número telefônico. O objetivo é se passar pelo usuário original do aplicativo para pedir empréstimos aos seus conhecidos e familiares ou, também, para obter informações íntimas ou confidenciais.

DICA DE SEGURANÇA

❑ Desconfie de conversas com pessoas cujos números de telefone não estejam salvos em sua agenda. Caso você receba mensagem de algum contato solicitando empréstimo de dinheiro ou depósito de algum valor em determinada conta, confirme com a pessoa a veracidade dessa solicitação. E, caso seja verdade, antes de qualquer confirmação de depósito, verifique os dados do destinatário (nome, CPF e agência bancária).

❑ Faça a configuração da foto do perfil para definir por quem ela pode ser vista. Abra o **WhatsApp** e **toque em Menu (os três pontinhos no canto superior da tela) > a seguir, toque em Configurações > clique em Conta** > **Privacidade e por fim > em Foto do perfil > toque na opção para permitir quem verá sua foto de perfil** > **se todos os usuários, se apenas os seus contatos (sugerido) ou se ninguém.**

TRT-11ª REGIÃO
Amazonas e Roraima

WHATSAPP

COMO ACONTECEM OS GOLPES?

❑ Os golpistas têm diversos meios de conseguir o número de telefone da vítima. Contudo, o mais usual é que seja obtido de anúncios em plataformas de sites de compras ou anúncios públicos em redes sociais (que abrangem não só os contatos da vítima). O golpista identifica que o usuário original do aplicativo fez um anúncio em algum tipo de site ou serviço da internet no qual o número de telefone é exibido para fins de transação comercial.

❑ A vítima recebe SMS do qual consta um código de 6 dígitos. O golpista se passa por funcionário da plataforma de anúncio e solicita o código alegando que isso é necessário para ativar o anúncio. O código, entretanto, foi enviado pela própria empresa **WhatsApp** ao usuário original do aplicativo, atendendo comando realizado pelo criminoso, a partir do momento em que deu início ao processo de transferência do **WhatsApp**, sem possuir a capacidade de receber a mensagem de SMS contendo o respectivo código. Este código é uma verificação do **WhatsApp**, ou seja, o golpista digitou o número de celular da vítima no celular dele para ativar o **WhatsApp**.

É por esse motivo que ele solicita o código, afirmando que isso seria necessário para habilitar o anúncio, induzindo a vítima a fornecê-lo. De posse desse código, o golpista desvia o **WhatsApp** da vítima para o aplicativo instalado no celular dele, e a vítima perde o acesso ao aplicativo. Após isso, o criminoso inicia conversas com amigos da vítima, fazendo-se passar por ela, alegando estar sem dinheiro, com algum problema na conta bancária ou com cartão de crédito bloqueado, e solicita valores emprestados, comprometendo-se a pagar no dia seguinte. Os amigos da vítima, acreditando tratar-se da pessoa, acabam transferindo o dinheiro para a conta bancária informada, que, normalmente, é de algum "laranja". Assim que a transferência é efetuada, eles também se tornam vítimas do golpe.

WHATSAPP

BURLANDO A AUTENTICAÇÃO DE DOIS FATORES

Para conseguir burlar o código de autenticação em duas etapas, o criminoso encerra a chamada como membro do Ministério da Saúde. Logo em seguida, o grupo realiza outra ligação para a vítima, mas fingindo ser o suporte do **WhatsApp**. Os **cibercriminosos** dizem que encontraram um atividade suspeita na conta da vítima. Em seguida, os hackers instruem o usuário a entrar em seu e-mail para resetar o código de autenticação em duas etapas e garantir mais segurança para o perfil. Os **cibercriminosos** utilizam as informações da vítima para solicitar ao **WhatsApp** que o código de verificação em duas etapas seja alterado na conta. Ou seja, o e-mail enviado para a vítima vem realmente dos responsáveis pelo aplicativo. **"Tanto a mensagem quanto o link para recuperar a dupla autenticação são legítimos, ou seja, foram enviados pela dona do aplicativo"**, comenta **Fabio Assolini**, especialista da **Kaspersky.Caso** o usuário prossiga com o reset do código de autenticação em duas etapas, a conta ficará insegura até que a nova senha seja configurada, o que abre uma pequena brecha para os **cibercriminosos** tomarem o perfil durante o reset do código de autenticação.

Para garantir que o golpe seja concluído, os hackers costumam ficar conversando com a vítima durante todo o procedimento, explica a **Kaspersky**. De acordo com Fabio Assolini, os **cibercriminosos** atingiram outro nível de engenharia social, o que cria novos desafios de segurança para o **WhatsaApp**. **"O aplicativo deve melhorar o processo de recuperação da dupla autenticação permitindo o recadastro na própria página da empresa, em vez de realizar a desativação"**, explica o especialista. **"Desta forma, este esquema seria inviabilizado."**

COMO SE PROTEGER

Como a principal arma utilizada pelos **cibercriminosos** é a engenharia social, **a principal dica para se proteger contra os golpes de roubo do WhatsApp é ficar atento.. Desconfie ao receber ligações desconhecidas e não compartilhe códigos de autenticação enviados via SMS.** Além disso, **mantenha a autenticação em duas etapas ativada no WhatsApp**. Por fim, **desconfie de ligações não solicitadas envolvendo supostos funcionários do app. "A plataforma de Mark Zuckerberg não costuma ligar para usuários em casos de problemas e o suporte oficial funciona pela web"**.

FACEBOOK

PREVENÇÃO: COMO EVITAR UM POSSÍVEL GOLPE

AUTENTICAÇÃO DE DOIS FATORES é assim que é chamada a autenticação em duas etapas do **Facebook**. É aconselhável que você troque sua senha. Para isso você tem de se lembrar da senha atual e ao escolher uma nova senha que esta seja considerada forte. Geralmente se utiliza o aplicativo no celular, porém é bem similar no computador. As etapas são as seguintes:

No lado direito superior toque nos 03 tracinhos (navegue para baixo) > Configurações e Privacidade > Configurações (navegue para baixo) > Segurança e Login (navegue para baixo) > Login – alterar senha. Após ter configurado uma nova senha, será perguntado se você deseja permanecer no aplicativo, opte que sim. Depois realize os demais passos:

Usar **AUTENTICAÇÃO DE DOIS FATORES** > **Mensagem de texto SMS (essa é opção mais simples a ser utilizada) > Confirme sua senha no Facebook.**

TRT-11ª REGIÃO
Amazonas e Roraima

FACEBOOK

INFORMAÇÕES

É uma das maiores fontes de informação utilizadas pela engenharia social. Por motivos diversos, são publicadas informações valiosas sobre comportamentos, hábitos, estados de espírito e momentos de vida que podem ser utilizados de forma escusa por pessoas mal-intencionadas. É a privacidade exposta ao mundo virtual. Por isso, deve-se ter muito cuidado com o que é postado.

COMO SE PROTEGER

- ❑ Configure a verificação em duas etapas.
- ❑ Controle o conteúdo daquilo que publica.
- ❑ Não torne públicas informações de natureza pessoal, como parentescos, RG, CPF, número de telefone.
- ❑ Evite fotos e vídeos pessoais e com familiares que informem que, naquele instante, estão fora de casa, que possam identificar residência ou locais de trabalho ou, ainda, que identifiquem onde você ou familiares estudam ou trabalham (uniforme).
- ❑ Verifique sempre as sessões ativas do seu aplicativo.
- ❑ Desabilite a permissão de aplicativos de terceiros.
- ❑ Tenha atenção quanto a jogos e páginas pelo Facebook e cuidado com cadastros e acesso a informações.
- ❑ Verifique quais aplicativos e sites utilizam os dados do Facebook para acesso. Exclua os que não são necessários. Para verificar, acesse **Configurações > Aplicativos e Sites > Ativos.**

TRT-11ª REGIÃO
Amazonas e Roraima

INSTAGRAM

PREVENÇÃO: COMO EVITAR UM POSSÍVEL GOLPE

AUTENTICAÇÃO DE DOIS FATORES Acesse seu perfil e vá **no lado direito superior toque nos 03 tracinhos > (navegue para baixo) > Configurações > Segurança > Segurança de Login > Autenticação de dois Fatores > usar Autenticação de dois fatores. O aplicativo solicitará o código de segurança de confirmação e você poderá confirmar por SMS ou por aplicativo de autenticação.**

COMO SE PROTEGER

- ❑ Configure a verificação em duas etapas.
- ❑ Por padrão, qualquer pessoa pode ver seu perfil e publicações no **Instagram**. Você pode tornar sua conta privada para que apenas os seguidores aprovados consigam ver o que compartilha. Caso sua conta esteja configurada como privada, somente os seguidores aprovados verão suas fotos ou vídeos. **Para configurar, vá a Configurações > Privacidade > Privacidade da Conta > Conta Privada.**
- ❑ Não mostre o status da atividade, que informa quando o usuário esteve on-line.
- ❑ Oculte story de pessoas que te seguem e que você não deseja que vejam suas publicações.
- ❑ Não permita compartilhamento de story.

INSTAGRAM

INFORMAÇÕES

Como o **Facebook**, o **Instagram** tem potencial de expor o usuário ao mundo virtual. Da mesma forma, tem-se tornado grande fonte de dados para a engenharia social, o que enseja as mesmas preocupações e cuidados com a proteção dos dados pessoais.

O golpe mais comum é a clonagem de perfil do usuário. Com capturas de tela das fotos postadas, os criminosos passam-se pela vítima, criam uma conta com nome de usuário parecido e dizem ter sofrido um "ataque hacker" no perfil original. Assim, solicitam novo contato para seguir amigos e familiares da vítima. Aproveitando-se da boa vontade deles, passam a enviar mensagens diretas, pedindo depósitos em dinheiro em conta bancária ou de outro tipo de instituição financeira, como, por exemplo, o **PayPal**, alegando ter perdido o acesso às contas em redes sociais e ao aplicativo do banco.

Outra forma de ação dos golpistas consiste em utilizar as imagens publicadas no **Instagram** para criar contas supostamente originais, que são usadas com o intuito de atrair potenciais compradores para os materiais postados em páginas fraudulentas ou de conteúdo pornográfico.

INSTAGRAM

O QUE FAZER QUANDO O APLICATIVO É CLONADO?

O golpe acontece geralmente quando o usuário possui muitos seguidores, e o golpista, usando a engenharia social, apropria-se da conta da vítima e passa a pedir resgate por ela.

Caso um usuário tenha perdido seu acesso ao **Instagram**, deverá, primeiramente, tentar reavê-lo via **Facebook** ou SMS. Além disso, é possível acessar a conta de e-mail vinculada ao aplicativo e localizar a mensagem que informa a modificação. Desfaça, caso possível, a modificação de senha.

DICA DE SEGURANÇA

- ❑ Configure a verificação em duas etapas.
- ❑ Use senha distinta para acessar o **Instagram** e o e-mail vinculado.
- ❑ Em caso de invasão criminosa, registre boletim de ocorrência na Polícia Civil.

TRT-11ª REGIÃO
Amazonas e Roraima

PIX

PIX é um novo meio de pagamento instantâneo, criado pelo Banco Central para ser uma nova opção, ao lado de TED, DOC e cartões, para que pessoas e empresas possam fazer transferências de valores, realizar ou receber pagamentos durante 24 horas por dia, inclusive em fins de semana e feriados.

Apesar de o funcionamento do **PIX** ter inIciado em 16 de novembro de 2020, vários golpes começaram a ser praticados bem antes, principalmente na forma de **phishing**. O objetivo é coletar dados bancários e pessoais, como senhas bancárias e números de CPF e celular. Os ataques de **phishing** imitam campanhas legítimas de bancos e **fintechs** (empresas de tecnologia focadas no mercado financeiro, com serviços exclusivamente digitais), em que são enviados links ou e-mails fraudulentos para que o usuário acesse página falsa e cadastre seus dados.

DICA DE SEGURANÇA

❑ Observe com cuidado todo o endereço eletrônico.

❑ Existem algumas precauções que você pode tomar para garantir a segurança da sua navegação. Se você acessar um site e desconfiar dele, verifique se há um ícone de cadeado em algum lugar. Para ser confiável, o site deve ter o cadeado.

Não digite seus dados em sites que não possuam esse ícone. Outro local para verificar a existência do cadeado é ao lado da URL da página. Ao clicar nele, será exibido o certificado de segurança.

❑ No site **www.whois.net**, você pode verificar as informações de registro do site.

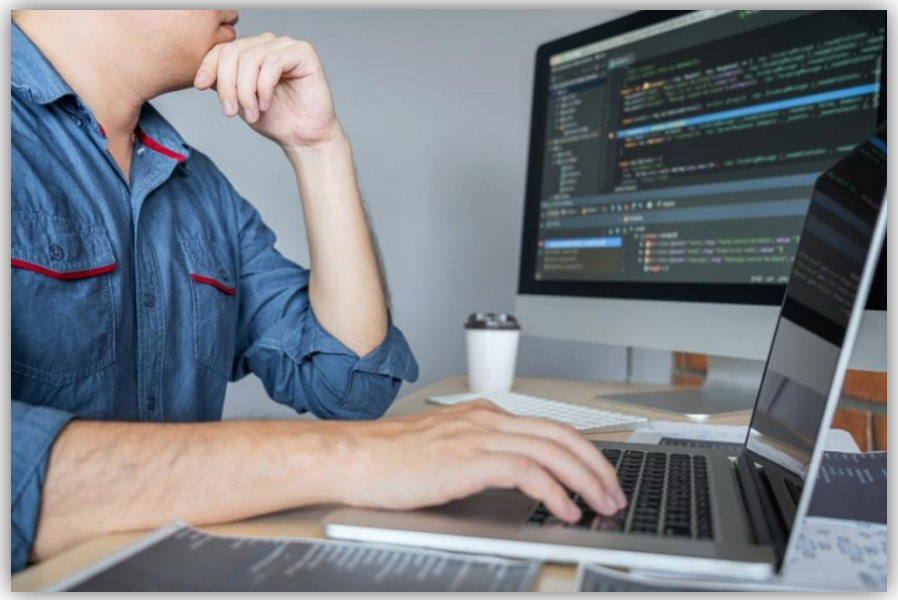
❑ Pesquise a reputação da empresa eletrônica em que pretenda efetuar a compra.

❑ Desconfie de objetos que estejam à venda por preço muito abaixo daquele praticado no mercado.

TRT-11ª REGIÃO
Amazonas e Roraima

SITES FALSOS

É comum abrir o navegador e, por equívoco, digitar incorretamente o nome do domínio que se pretenda acessar. Aproveitando-se dessa corriqueira situação, os criminosos, para enganar os usuários, criam site fraudulento, praticamente idêntico ao site verdadeiro, de venda de mercadoria (eletrônicos, eletrodomésticos, etc.). Esse golpe costuma ter maior incidência em datas comemorativas e promocionais, como, por exemplo, na **black friday**. O golpista usa endereços de empresas famosas, alterando só o final do endereço.



DICA DE SEGURANÇA

- ❑ Não clique em links desconhecidos.
- ❑ Nunca forneça códigos solicitados por SMS.
- ❑ Use os canais oficiais do seu banco ou agente financeiro para saber mais sobre o PIX. Somente cadastre-se pelos meios indicados por eles.
- ❑ De forma geral, empresas nunca pedem que os usuários forneçam suas senhas via e-mail, ou seja, bancos, instituições financeiras e operadoras de cartão não vão pedir esse dado. Desconfie de pedidos de dados sigilosos por e-mail.
- ❑ Não instale programas nem baixe arquivos em anexos enviados por lojas ou estabelecimentos.
- ❑ Na dúvida, contate seu gerente bancário.

TRT-11ª REGIÃO
Amazonas e Roraima

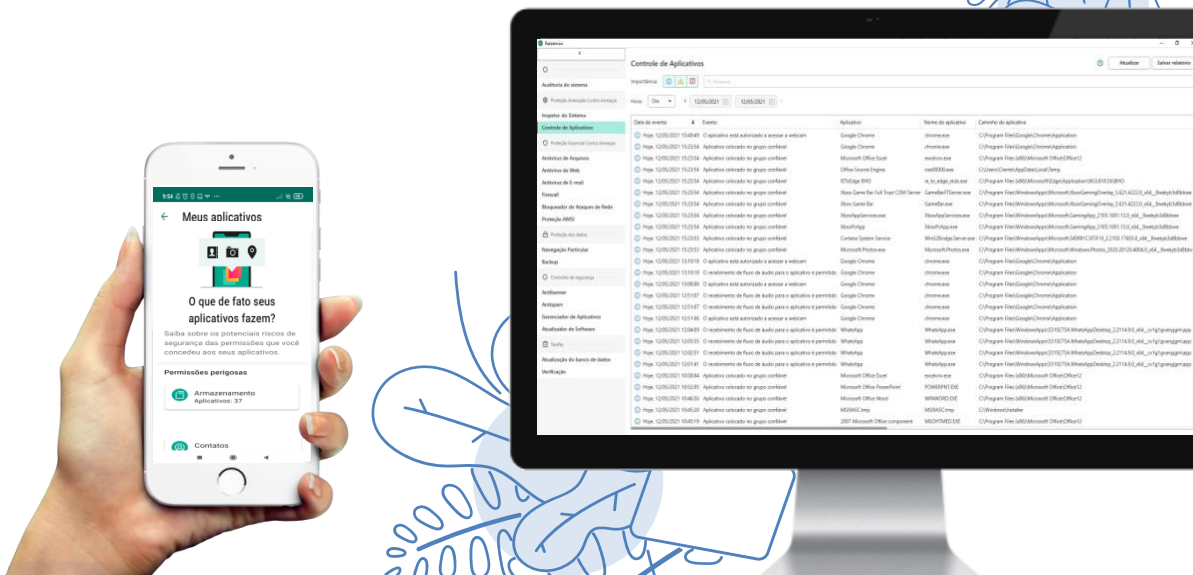
COMPUTADOR E DISPOSITIVOS MÓVEIS

COMO PROCEDER

❑ **Mantenha** seu **computador** e **dispositivos móveis seguros**, com versão mais recentes de todos os programas instalados, com todas as **atualizações aplicadas**.

❑ Utilize e mantenha **atualizados** mecanismos de segurança, como **antivírus** e **firewall pessoal**.

❑ Mantenha controle sobre seus dispositivos principalmente em locais de risco, não deixa sobre a mesa, cuidado com bolsos e bolsa em ambientes públicos.



TRT-11ª REGIÃO
Amazonas e Roraima

BOATOS

Boato é **"uma notícia de fonte desconhecida, muitas vezes infundada, que se divulga entre o público"**. Se após verificada, a notícia for considerada verdadeira diz-se que o boato foi confirmado e, caso contrário, que ele foi desmentido.

Como não se conhece a fonte da notícia não é possível saber exatamente o motivo pelo qual ela foi criada, podendo variar de simples diversão até interesse políticos e econômicos.

Para circularem, os boatos contam com a ajuda de contas falsas automatizadas e da boa vontade das pessoas que os repassam.

As notícias que são disseminadas como boatos na internet podem prejudicar a segurança dos usuários. Por quê? Em muitos casos, as notícias são ou contêm vírus que interferem na conexão e causam danos ao sistema do seu aparelho eletrônico, seja ele **computador**, **smartphone**, **tablet**, **entre outros**.

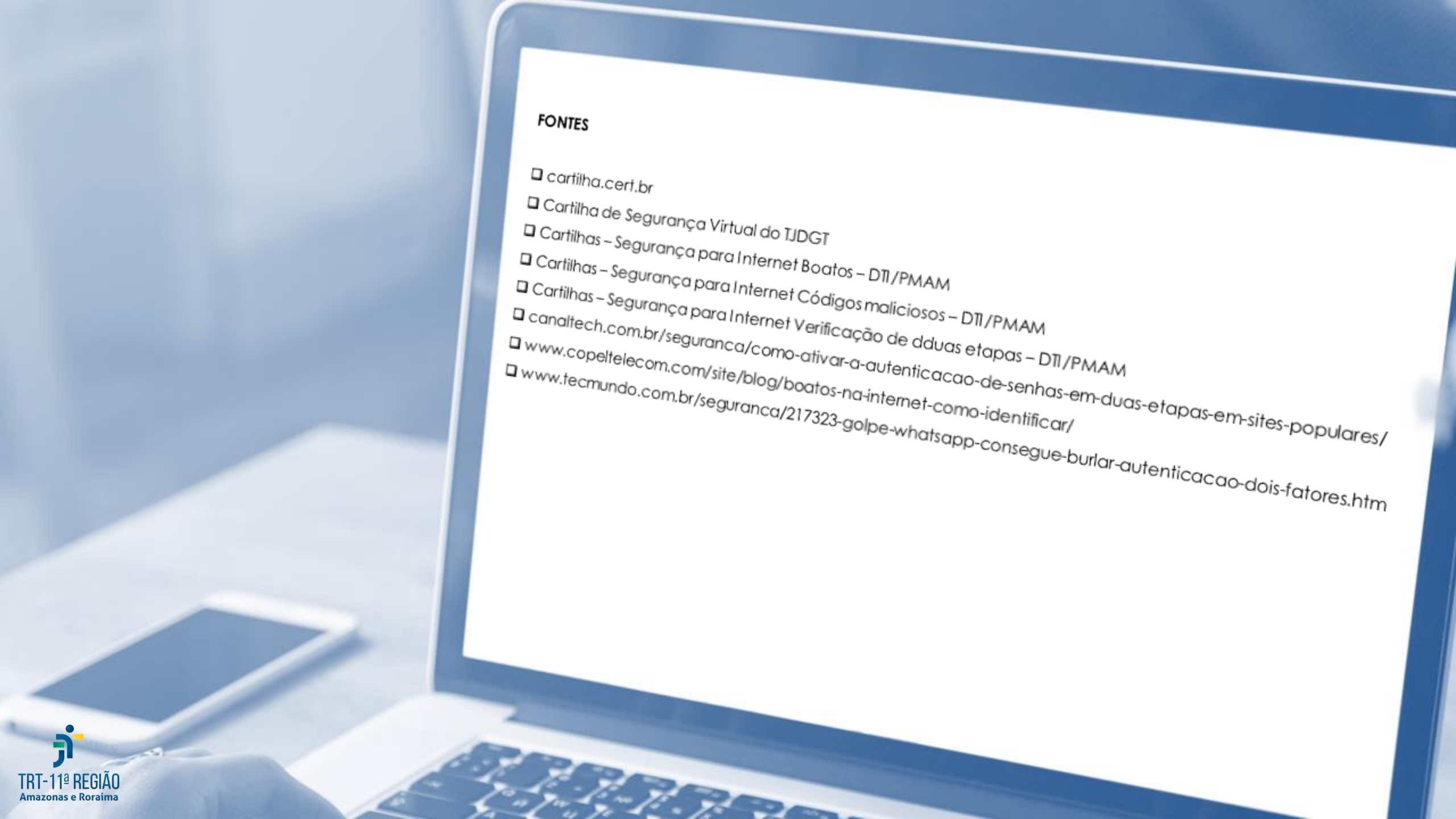
Por isso, além de sempre buscar saber se determinadas notícias são verdadeiras ou não, é aconselhável evitar acessá-las em sites suspeitos, que não apresentam os **quesitos necessários de segurança na internet**.

COMO PROCEDER

❑ Digamos que você recebeu uma mensagem no **Whatsapp** sobre um inseto que está disseminando uma doença mortal desenfreada no mundo inteiro. Ele saiu de outro país, atravessou oceanos, está se proliferando rapidamente e você precisa ajudar a conscientizar a sociedade sobre o assunto.

❑ Bom, antes de compartilhar uma notícia como a do exemplo acima, dá uma olhada nos sites: **Boatos.org**, **e-farsas.com** ou **verdadeabsoluta.com**. Neles, você encontra várias notícias explicando sobre insetos mortais, doenças alarmantes, acontecimentos surreais, eventos catastróficos, entre outros boatos que geralmente são compartilhados pelas pessoas. Na maioria dos casos, é só um alarme falso e falta de informação e pesquisa.

TRT-11ª REGIÃO
Amazonas e Roraima



TRT-11ª REGIÃO
Amazonas e Roraima

COMISSÃO DE SEGURANÇA

CRIADA EM 14 DE OUTUBRO DE 2015


TRT-11ª REGIÃO
Amazonas e Roraima