- GUIA -

SEGURANÇA DIGITAL

REPÓRTERES SEM FRONTEIRAS

Imagem de Free-Photos por Pixabay

REPORTERES SEM FRONTEIRAS
PELA LIBERDADE DA INFORMAÇÃO

Os jornalistas tornaram-se um alvo preferencial de ataques por grupos disseminadores de ódio, principalmente na internet. Nesse tenso contexto de trabalho, a RSF lança o Guia de Segurança Digital para auxiliar o trabalho de jornalistas, com dicas básicas de como prevenir casos de ataques e proteger suas comunicações. Ataques direcionados a portais de notícias, vazamento de informações pessoais de jornalistas e invasão de sistemas são exemplos de casos em que comunicadores tiveram sua segurança digital violada. O Guia foi pensado com o objetivo de trazer orientações simples que ajudam a prevenir esse tipo de violência.

> Encriptação total pode chamar a atenção desnecessariamente

Algumas dicas do Guia são recomendadas apenas para situações específicas, quando estiver trabalhando com informações e fontes sensíveis. Optar por estar permanentemente camuflado pode passar a impressão de um comportamento suspeito

SUMÁRIO

REPÓRTERES SEM FRONTEIRAS

COMO PROTEGER OS MEUS DISPOSITIVOS?

No século XXI, grande parte do trabalho de um comunicador está armazenado em dispositivos eletrônicos. Notebooks, computadores, smartphones e tablets são ferramentas indispensáveis na vida de um jornalista, por isso é necessário proteger esses aparelhos de qualquer tipo de ameaça.

Imagem de Free-Photos por Pixabay

Nunca ignore uma notificação do sistema de antivírus ou de atualizações de sistema operacional seu dispositivo.

#dicas:

1. Mantenha o firewall e antivírus dos seus dispositivos sempre atualizados e ativos.

2. Evite instalar aplicativos e softwares desnecessários, e caso for fazer, leia atentamente as permissões de acesso requeridas. Instale apenas aplicações seguras e bem avaliadas por usuários.

3. Dê preferência para aplicativos e softwares de código livre e que recebam atualizações constantemente. Além disso, nunca permita aos apps o acesso à câmera e ao microfone do seu dispositivo (exceto em casos que o app precisa dessas ferramentas para o funcionamento).

4. Evite armazenar informações sensíveis no seu smartphone e realizar conversas sigilosas pelo celular. Se necessário, você pode usar ferramentas que não utilizam a rede de telefonia, como o Signal, um aplicativo que trabalha através da rede de dados.

5. Sempre bloqueie a tela dos seus dispositivos, utilize um ou mais tipos de validação de desbloqueio e defina senhas fortes. Além disso, não se esqueça de se desconectar das suas contas quando não estiver usando o serviço.

6. Em reuniões que envolvam informações particularmente sigilosas, evite a presença de aparelhos celulares na mesma sala.

A SENHA É A PRIMEIRA BARREIRA

A senha é o primeiro passo para a uma verificação de segurança. A definição de uma senha forte pode salvar os seus arquivos e evitar invasões ou perdas de informações e/ou dispositivos.

Imagem de TheDigitalWay por Pixabay

Use senhas diferentes em cada conta, caso contrário, você vai arriscar todas as contas em uma possível invasão. Se você acha que pode esquecer as senhas, use aplicativos para gestão de senhas, como o Keepass e o Dashlane!

#dicas:

1. Use frases completas como senhas, isso pode dificultar o trabalho de hackers e softwares que tentem invadir seu sistema.

2. Utilize siglas de frases para aumentar a força da sua senha.
Ex.: Fui embora de Santa Catarina no dia 15!
➡ FedSCnd15!

3. Use geradores de senha para criar senhas fortes automaticamente, como o **Safepass.**

4. Verifique a força da sua senha com ferramentas como o site ***"How Secure is My Password?"*** que calcula o tempo em que um sistema hacker demoraria para descobrir sua senha.

Imagem de Jacqueline Macou por Pixabay

COMO CUIDAR DAS MINHAS MÍDIAS PORTÁTEIS?

Dispositivos e mídias portáteis podem ser de grande ajuda na rotina de trabalho, no armazenamento de informações ou no transporte de arquivos. Entretanto, essas mídias também podem atuar como uma porta de entrada para vírus e ameaças no seu sistema.

Nunca conecte uma mídia ou dispositivo que você desconhece a procedência no seu aparelho.

#dicas:

1. Altere as configurações do seu pen-drive/ dispositivo de armazenamento para evitar ameaças sem precisar instalar programas. Essa configuração da propriedade de segurança do dispositivo bloqueia ações de malwares caso o computador utilizado esteja infectado. Confira o tutorial.

2. Quando adquirir uma nova mídia, não esqueça de encriptografar o dispositivo. Você pode utilizar ferramentas como o *Rohos Mini Drive*.

3. Quando utilizar computadores que não são um dos seus, carregue no seu pendrive ou hd um software portátil anti spyware, como o SUPERAntiSpyware Portable Scanner.

4. Nunca deixe de atualizar o sistema antivírus do seu computador ou ferramenta de trabalho, evite que o possível contágio da sua mídia atinja também outros dispositivos.

NAVEGAR COM SEGURANÇA

A internet é uma grande fonte de informações e facilita muito a vida de jornalistas. Entretanto, é necessário ficar atento aos riscos que o mundo on-line oferece, uma simples conexão ou download suspeito podem colocar em risco a sua segurança digital.

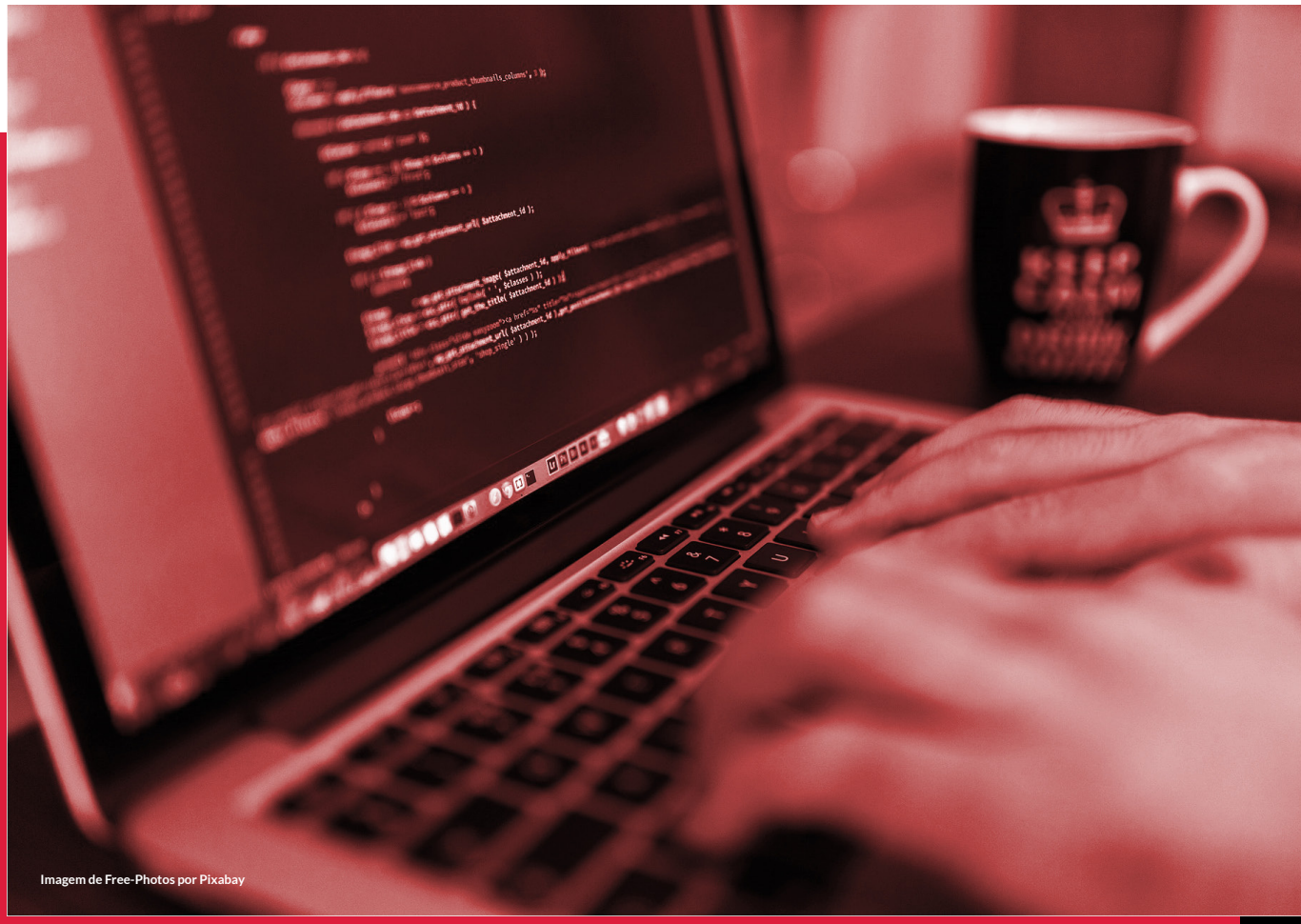

Imagem de Free-Photos por Pixabay

Ao navegar em um site, verifique se há presença do prefixo de segurança “https://” na barra de endereços, ele garante uma maior proteção na transmissão de dados.
Não confie em sites sem esse prefixo.

#dicas:

1. Instale um programa de VPN (Virtual Privative Netwok ou no português Rede Privada Virtual) que garante a segurança dos seus dados através de canal de comunicação virtual protegido por senhas e criptografia.

2. Use a ferramenta TOR quando precisar de descrição. O TOR é um software de código aberto que protege a identidade e privacidade dos usuários enquanto estão on-line. Ele oculta a sua identidade na rede e impede que qualquer interessado visualize as suas tarefas.

3. Cuidado ao acessar redes Wi-Fi abertas. A conexão desses locais pode não ser totalmente segura, por isso não acesse dados confidenciais de trabalho ou bancário enquanto estiver conectado nessas redes. Sempre utilize VPN nas redes abertas e nunca deixe de ativar a opção “esquecer a rede” depois se desconectar.

4. Não se engane com anúncios de promoções ou serviços gratuitos, bloqueie pop-ups e evite fazer cadastros com informações pessoais em campanhas publicitárias.

5. Não armazene senhas no navegador. Caso contrário, se alguém tiver acesso ao seu dispositivo, terá acesso a suas senhas facilmente. Lembre-se sempre de se desconectar de contas e redes sociais, além de limpar o histórico do browser e cookies.

Imagem de Pixelkult por Pixabay

OS RISCOS DAS REDES SOCIAIS

As redes podem ser de grande ajuda para o trabalho de um comunicador, mas também podem oferecer demasiada exposição de dados pessoais e intimidade de jornalistas. Fique atento com o que você compartilha nas redes sociais, nunca sabemos até quem determinada informação pode chegar.

Separe o conteúdo profissional do conteúdo pessoal. Configure sua conta para que o conteúdo pessoal seja exibido somente para pessoas que você confie.

#dicas:

1. Não aceite pedido de amizade de contatos desconhecidos nas suas redes, e delete os contatos desconhecidos/ suspeitos já existentes.

2. Troque sua senha com frequência: ao menos uma vez a cada 3 meses. E quando for redefini-la, não esqueça de utilizar uma senha forte.

3. Não utilize sua conta de rede social para fazer cadastros em outros sites.

4. Desconecte aplicativos que acessem suas informações pessoais e utilizam seu perfil em redes sociais.
Ex.: Facebook (Configurações > Aplicativos e sites > Selecione o aplicativo > Remover).

5. Remova sua conta de outros dispositivos.
Ex.: Facebook (Configurações > Segurança > “Onde você está conectado” > Editar > Selecione a sessão ativa > Encerrar).

6. Desabilite a opção “Compartilhar localização” com as redes sociais do seu celular.

Imagem de Gabrielle_cc por Pixabay

CUIDADOS COM O E-MAIL

O e-mail é uma ferramenta que contribui muito no trabalho de jornalistas e comunicadores. Apesar de oferecer muitas facilidades, as contas de troca de mensagens e informações on-line também pode ser uma porta de entrada para vírus, ameaças e fishing.

Nunca faça download ou clique em links de remetentes desconhecidos, ao acessar um arquivo suspeito você pode pôr em risco todas as informações da sua conta e do seu dispositivo.

#dicas:

1. Habilite a autenticação de dois fatores para uma dupla verificação de segurança em todas as suas contas. Isso reforça a proteção no momento de login do seu e-mail.

2. Não confie em e-mails de origem desconhecida, em caso de remetentes corporativos, pesquise o e-mail no site da empresa para garantir a veracidade da conta.

3. Em caso de dúvidas, utilize ferramentas como o ***Vírus Total***, um scanner on-line que verifica a presença de vírus.

4. Utilize ferramentas de e-mail criptografado para enviar informações mais sensíveis, como o ***ProtonMail*** ou as **chaves PGP**.

5. Verifique se seu endereço de e-mail já foi pirateado no site "**Have I Been Pwned?**".

COMO ME ORGANIZAR EM VIAGENS?

Em viagens a trabalho, é necessário o dobro de cuidado com suas informações e equipamento. Não confie em terceiros e evite ficar longe do seu material de trabalho.

Imagem de Rudy and Peter Skitterians por Pixabay

Evite viajar carregando informações sensíveis e desnecessárias para o trabalho que irá fazer. Não coloque em risco informações que você não utilizará em determinado período de tempo.

#dicas:

1. Antes de qualquer tipo de viagem, pesquise características de segurança do local. Avalie os riscos e organize seus dispositivos. Não carregue materiais ou informações que possam ser considerados ilegais ou ofensivos no destino.

2. Durante a viagem, faça sempre backup dos seus arquivos para o caso do seu equipamento ser confiscado, roubado ou perdido.

3. Faça a encriptação do seu equipamento e garanta que ele tenha um programa de VPN operacional.

4. Use acessórios de segurança no seu computador, como um filtro de privacidade de telas e marcadores de identificação, além de usar somente as suas próprias chaves USB e nunca permitir que alguém carregue a bateria do celular no seu computador.

5. Planeje e estabeleça uma chamada de segurança diariamente com o seu/sua editor/a, e avise imediatamente a redação caso o seu equipamento seja confiscado, roubado ou perdido.

6. Mantenha seu material de trabalho sempre com você, e caso necessite deixar o seu celular temporariamente, leve consigo o chip.

#saiba mais

> Confira recomendações da RSF extraídas do relatório "*Assédio online de jornalistas: quando os trolls atacam*".

> Em caso de emergência ou ataque, acesse a pagina ***Help Line*** da organização ***Access Now***.

Photo by @NahashonDiaz from nappy.co

REPÓRTERES SEM FRONTEIRAS trabalha pela liberdade, independência e pluralismo do jornalismo em todo o planeta. Com status consultivo na ONU e na UNESCO, a organização com sede em Paris tem 14 escritórios em todo o mundo e correspondentes em 130 países.

Secretário Geral: **CHRISTOPHE DELOIRE**

Autores: **LETHICIA AMÂNCIO DE ALMEIDA** /
ESCRITÓRIO RSF AMÉRICA LATINA

SECRETARIA INTERNACIONAL
CS 90247 75083 PARIS CEDEX 02
TEL. +33 1 44 83 84 84
WEB: WWW.RSF.ORG

REPORTERES
SEM FRONTEIRAS
PELA LIBERDADE DA INFORMAÇÃO