BIM
Boletim Informativo Mensal
Comunicar para Educar
Janeiro/2022 – Ano 3 – nº 24

Você já teve problemas com pessoas se passando por você nas suas redes sociais?

Caso a resposta seja sim, você pode estar sendo alvo de perfil falso (*fake*).

Na atualidade é difícil conhecer uma pessoa ou empresa que não esteja presente em mídias sociais, pois são meios essenciais para interagir com pessoas e agregar relacionamentos interpessoais e profissionais.

O aumento da popularidade em perfis nas redes sociais aumenta o perigo de cair em golpes *online* praticados por cibercriminosos. Sendo assim, aprender a utilizar esses canais com segurança é relevante para manter sua privacidade e confiabilidade nas informações disponibilizadas.

Os problemas relacionados à segurança nessas redes são frequentes. Com isso, os possíveis danos materiais e de imagem são mais comuns do que imaginamos.

Normalmente, os cibercriminosos conseguem acesso a uma conta porque a senha é fácil, pode ter sido utilizada em outro serviço ou vazou. Existe, também, a possibilidade de algum aplicativo malicioso que esteja conectado a sua conta ter permissão de acessar seu perfil e mensagens, tendo acesso a dados pessoais ou mesmo a sua senha.

Os usuários podem observar algumas dicas básicas, do que fazer e do que não fazer, para manter a sua conta segura.

- Criar senha forte. Quanto maior for a senha e quanto maior a variedade de caracteres (letras minúsculas e maiúsculas, números e caracteres especiais, como !@#), maior a segurança contra ataques de sequestro de senha. A senha não deve incluir nenhuma informação pessoal do usuário, como endereço ou número de telefone. Também é melhor não incluir nenhuma informação que possa ser acessada nas redes sociais, como nomes de crianças ou animais de estimação, e não deve conter letras ou números consecutivos [1].

- Usar uma senha para cada site. É uma boa prática utilizar senhas diferentes para cada conta. Utilize um gerenciador de senhas para ajudar a guardar as senhas de aplicativos e sites que você gerou ou criou. Existem diversas opções gratuitas e pagas, só é preciso entender qual delas corresponde a suas expectativas.

- Ativar a autenticação de dois fatores. Habilite a autenticação do dispositivo, a autenticação de dois fatores (2FA). Para proteção máxima, habilite o uso de autenticação biométrica (face ou impressão digital). O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo publicou a Recomendação 11/2021 sobre Dispositivos Móveis, onde recomenda como uma das medidas protetivas, ativar a autenticação de dois fatores para aplicativos ou sites que a suportam [2].

- Configurar a opção de receber alertas de *login* em sua conta. Esta configuração é relevante para alertar quando uma pessoa acessar sua conta; caso avalie que houve acesso indevido, faça alteração de senha para evitar problemas em sua conta.

- Sair da Rede Social em computadores públicos. Caso tenha que acessar a rede social em um computador que não seja o seu próprio, é relevante que faça *logout* (clique em Sair) quando não for mais usar sua conta. Dessa forma, não corre o risco de a próxima pessoa que usar o computador utilizar sua conta e fazer publicações fazendo-se passar por você.

- Escolher amigos de confiança. A maioria dos aplicativos de redes sociais oferecem a opção de escolher um número de amigos para ficarem cada um com um código de segurança diferente. Sendo assim, se você perder o acesso à conta, poderá pedir o código a um dos amigos e conseguir acessar seu perfil, mesmo que alguém malicioso tenha mudado sua senha.

- Observar as extensões e/ou programas instalados. Não menos importante, verifique extensões do seu navegador e programas mal-intencionados que podem existir no dispositivo computacional que esteja utilizando.

Fica a dica: prevenção nunca é demais!

REFERÊNCIAS

[1] https://www.security.org/how-secure-is-my-password/, acessado em 8 de dezembro de 2021.
[2] https://www.cisa.gov/sites/default/files/publications/CEG_Mobile%20Device%20Cybersecurty%20Checklist%20for%20Organizations.pdf, acessado em 9 de dezembro de 2021.

BIM
Boletim Informativo Mensal
Comunicar para Educar
Janeiro/2022 – Ano 3 – nº 24

Informação Classificada como SECRETA

Na edição anterior falamos da informação classificada no grau de sigilo RESERVADO. Agora falaremos da informação classificada no grau SECRETO.

Uma informação pode ser classificada como SECRETA quando for considerada imprescindível à segurança da sociedade, ou do Estado, levando em conta o risco, ou o dano à segurança, e o prazo.

O prazo máximo de classificação da informação SECRETA é de até 15 anos; o tempo é contado a partir de sua produção. As autoridades que possuem competência para classificar nesse grau são: os titulares de autarquias; os titulares de fundações ou de empresas públicas; e os titulares de sociedades de economia mista.

Os agentes públicos que classificam a informação no grau SECRETO, também têm competência para classificar as informações no grau RESERVADO.

Para saber mais sobre esse assunto acesse link: https://www.gov.br/gsi/pt-br/centrais-de-conteudo/publicacoes/legislacao/Lei_10683

Riscos da Exploração da Autoimagem na Internet

Com o advento das mídias sociais, o nível de **exploração da autoimagem** aumentou bastante. Podemos definir a autoimagem como o conhecimento e a representação que a pessoa tem sobre si mesma. Mas não para por aí. Desde o início das relações sociais, o homem busca a aprovação alheia, a fim de reforçar seu pertencimento a determinado grupo de indivíduos, levando-o a uma constante reflexão sobre sua autoimagem. No ambiente virtual, esse comportamento se amplificou e passou a representar um risco.

As postagens de viagens, relacionamentos e sucesso profissional são exemplos de atitudes de exploração de autoimagem e colaboram na construção da imagem que desejamos que o outro tenha de nós. Porém, devemos ter cuidado ao explorarmos a nossa autoimagem na internet. Alguém nesse ambiente, cujo objetivo seja o de se passar por uma outra pessoa ou espalhar notícias inverídicas, pode utilizar as imagens que nós mesmos fornecemos.

É importante ressaltar também que a exploração exacerbada da autoimagem possibilita que pessoas mal-intencionadas coletem informações pessoais sobre nós e rastreiem nossos hábitos, como locais que frequentamos, nossos horários, se temos filhos e quais são os nomes deles, dentre tantos outros dados que podem ser levantados, abrindo espaço para golpes, fraudes e sequestros.

Ao criar um perfil de uso pessoal, busque segurança. **Não publique**:

- **documentos e dados pessoais** - RG, CPF, carteira de habilitação e carteirinha da escola fazem parte da lista de documentos que devem ficar fora das mídias sociais;
- **dados financeiros** – número do banco, da agência, da conta corrente, da poupança e dos cartões não devem ser compartilhados; e
- **informações do local de trabalho** - não forneça o endereço, nem o horário de funcionamento, tão pouco os seus horários. E, não menos importante, não exponha as pessoas que trabalham com você e nem as rotinas dentro da organização.

Seja consciente e faça a sua parte! Proteja-se!

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: AssESI Sugestões: asscom.dsi@presidencia.gov.br