RECOMENDAÇÕES NA ÁREA DE SEGURANÇA INSTITUCIONAL

A Subprocuradoria-Geral de Justiça de Política Criminal Institucional e o Setor de Segurança Institucional[*], com apoio do *Cyber* Gaeco e do CTIC, apresentam dicas e sugestões para aprimorar a segurança no uso de aplicativos e de rede social (facebook).

I. APLICATIVOS DE MENSAGENS:

1. Ative a "verificação em duas etapas (ou dois fatores) em todos os aplicativos que possuir, em especial os de troca de mensagens instantâneas como whatsapp, telegram e outros similares;

2. Habilitar um e-mail de segurança;

3. Sempre feche as sessões abertas do whatsapp web, do telegrama web e outros similares, quando deixar o computador. Periodicamente verifique se há outros computadores estranhos com acesso indevido;

4. Jamais utilize senhas fáceis para o desbloqueio da tela do celular ou computador ou para qualquer outro aplicativo.

5. Ative o bloqueio automático da tela quando o celular permanecer ocioso por alguns minutos. Não saia de sua mesa de trabalho deixando o computador sem a sua vigilância e desbloqueado, permitindo o acesso de terceiros;

6. Habilitar o controle de acesso por *touch* ou reconhecimento facial;

7. Apague o histórico de conversas passadas, sempre que não forem mais úteis. Há formas de baixar o histórico de conversas e preservá-las em locais seguros (Icloud, Google Drive, Drop Box) ;

[*] http://www.mpsp.mp.br/portal/page/portal/Assessoria%20de%20Seguran%C3%A7a%20Institucional.

8. Evitar a mesma senha para mais de uma aplicação

9. Periodicamente, preste atenção para identificar se uma mensagem que você sabe que não leu está marcada como "lida";

10. Cuidado com e-mails suspeitos que pedem suas informações pessoais (*phishing*). Com informações pessoais, criminosos podem se passar por você e gerar novo chip de celular (SIM Swap);

11. Se perceber que ficou sem sinal da operadora – principalmente em uma área que você conhece e sabe que tem sinal – desconfie.

12. Não abra e não repasse fotos, links, vídeos e documentos cuja procedência desconhece, podem estar infectados com vírus, trojans ou outro malware.

Ficou em dúvida ainda? Procure no *google* ou no *youtube* como modificar a configuração de seu celular conforme o modelo e sistema operacional. Busque por palavras-chave como: duas etapas whatsapp iphone ou android.

II. USO DO FACEBOOK COM SEGURANÇA*:

1. **Alertas de login**: reiteramos o recurso do uso da autenticação em dois fatores. O facebook também dispõe dessa funcionalidade há tempos e basta que você ative as aprovações de login para desfrutar dela. Para ativá-la, entre: Configurações > Segurança e login, clique em Usar a autenticação de dois fatores **e** clique em Ativar. Por padrão, a senha de seis dígitos é enviada para o seu número de telefone, mas você pode configurar um aplicativo gerador de códigos procurando pela opção com este nome na mesma página;

2. **Chaves de segurança físicas:** Uma medida ainda mais eficaz para proteger a sua conta é a adoção de chaves de segurança físicas. Funciona assim: ao ativar as chaves de segurança na sua conta, você pode ativar as aprovações de login utilizando um dispositivo USB. Em outras palavras, só acessa a conta quem estiver com o dispositivo em mãos. Mas, há o inconveniente de que tais chaves

* Seguimos em grande parte as dicas dos sites, visitados em 16/6/19: https://canaltech.com.br/redes-sociais/seguranca-no-facebook-confira-7-dicas-para-se-manter-protegido-na-rede-social/ e https://tecnoblog.net/232718/seguranca-proteger-conta-facebook/ .

têm de ser adquiridas de outras empresas, como a Yubico, o que exige um custo adicional e, talvez, só valha a pena para donos de negócios e páginas grandes na rede.

3. **Adote senhas complexas:** reiteramos a necessidade de se evitar o uso de senhas simples, como 'senha', '123mudar' e coisas do tipo pelos incautos. Para evitar dores de cabeça nesse sentido, a recomendação é adotar uma senha que tenha pelo menos oito caracteres e usar uma combinação complexa que inclua números, letras e caracteres especiais. Evite incluir o seu nome ou palavras comuns. Quando mudar sua senha, fique atento ao indicador que mostra se sua senha é forte o suficiente ou não e tente combinar letras maiúsculas e minúsculas para dificultar ainda mais a vida dos hackers. E não se esqueça: o ideal é que cada senha que você usar seja única. Jamais use a mesma senha em mais de um serviço. Por fim, não use sua senha do Facebook em outro local online e nunca compartilhe sua senha.

4. **Contatos de confiança:** Outro recurso de segurança bastante interessante do Facebook são os contatos de confiança. Eles funcionam assim: caso você tenha algum problema com sua conta e não esteja conseguindo acessá-la por ter esquecido a senha e não conseguir enviar uma nova para o seu e-mail, são os contatos de confiança que são ativados para lhe ajudar nisso. Portanto, selecione-os com cautela para não passar por sufoco.

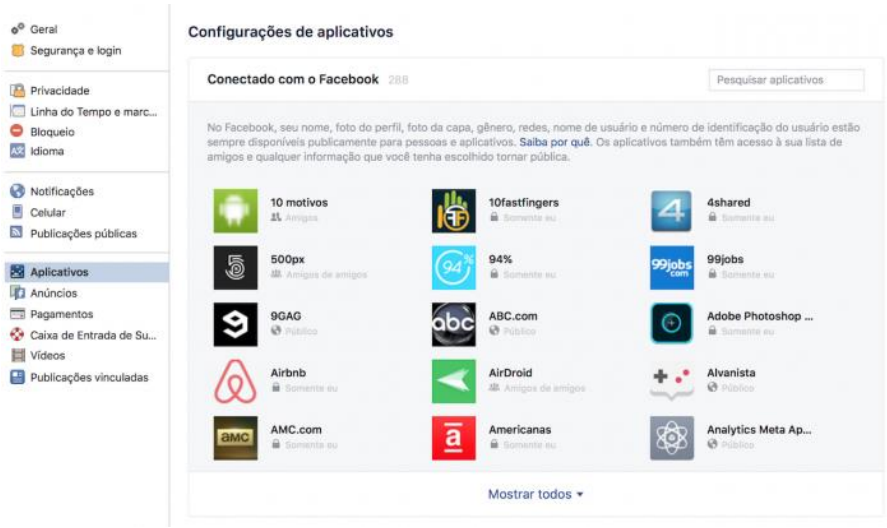
5. **Aprenda a lidar com spam:** A circulação de *spam* em grande quantidade é um dos problemas que afetam a segurança do Facebook. Com postagens sensacionalistas e links duvidosos, acaba sendo muito fácil cair numa cilada e deixar sua conta em risco. Quando isso acontece, geralmente você vai começar a ver sua conta criando publicações, eventos, grupos ou páginas sem o seu conhecimento. A dor de cabeça, porém, tem uma solução e ela é mais simples do que você pensa. Para resolver isso, verifique seu histórico de login e veja se não há acessos suspeitos em sua conta. Também execute uma análise das suas publicações e curtidas recentes e verifique o Registro de Atividades para excluir o conteúdo indesejado. Por fim, observe se não há nenhum serviço ou aplicativo escuso conectado à sua conta; em caso positivo, remova-o.

6. ***Phishing*:** Como dissemos no tópico anterior, a quantidade de links e notícias falsas que circulam no Facebook tem se tornado um problema para a rede social, que agora vem criando mecanismos para combater esse tipo de conteúdo. Enquanto as coisas não ficam 100% nesse aspecto, o ideal é que você fique atento para não ser vítima de *phishing*. O *phishing* é uma tentativa maliciosa de obter acesso à sua conta e aos seus dados pessoais e financeiros. Normalmente é uma prática associada à distribuição de links maliciosos e exibição de sites falsos que muito se assemelham aos oficiais. Nem sempre há erros de digitação e de grafia; assim, deve-se se atentar para outros detalhes,

como por exemplo, se confere com o padrão de conduta da instituição respectiva, se os links levam a destinos diferentes do local indicado nas publicações. Fique atento a tudo isso e caso tenha dúvidas a melhor saída é visitar o site oficial por sua conta, sem ser a partir do link que você clicou. Caso detecte alguma mensagem ou publicação falsa, você pode denunciá-la ao Facebook através do e-mail phish@fb.com ou nos links de denúncia que aparecem no site.

7. **Cuidado com quem vê seus posts:** Embora possa parecer simples, definir quem exatamente poderá ver suas publicações é uma das melhores maneiras de se resguardar *online* e evitar golpes de engenharia social. Portanto, sempre defina com critério a audiência de suas publicações para evitar maiores problemas.

8. **Veja quais apps controlam a sua conta:**



Na página acima você consegue ver os aplicativos que conectou ao Facebook e as permissões que foram concedidas a eles, além de sites que você fez login com a conta da rede social. É importante revisá-los para ter certeza do quê exatamente consegue, por exemplo, pegar sua lista de amigos ou informações básicas do perfil. Para controlar o acesso de cada app, clique no aplicativo desejado e depois em **Remover aplicativo**. Ou, caso não queira remover, apenas desmarque as informações fornecidas ao app.

9. **Seja discreto**: não revele seu local de residência e quem são seus familiares; embora seja algo que se possa descobrir de diversas formas, não facilite a vida daquele que tem motivos para querer saber sobre sua privacidade e intimidade; não revele que sua residência está sem ninguém, como, por exemplo, por meio

de fotos de viagens; não exponha seus filhos e os locais onde eles costumam frequentar, como escolas, etc.

III. SEGURANÇA BANCÁRIA:

1. O aplicativo que você baixa pelo *Apple Store* ou pelo *Google Store* é mais seguro que o uso pelo computador. Dê preferência a transações bancárias pelo celular do que pelo computador.

2. Nas transações por computador, habilitar segurança em dois fatores.

3. Crie um cartão de crédito para transações virtuais com outros limites. Atualmente todos os bancos emitem cartões voltados para transações pela *Internet*.

4. Troque as senhas padrão dos roteadores, por senhas pessoais. Há meios de invadir seu roteador.

5. Desconfie sempre de ligações telefônicas e de e-mails. Não forneça qualquer senha por telefone ou e-mail. Na dúvida entre em contato com seu banco por meio do próprio aplicativo do Banco.

6. Desconfie sempre de boletos enviados por e-mail. Sempre confira o remetente colocando o cursor em cima do e-mail do remetente. Nem sempre o que aparece escrito corresponde ao verdadeiro e-mail.

7. Atualmente é possível realizar ligações simulando ser outro número. Isso acontece com os números de telefone de bancos. Ligações de Banco sempre desconfiem.

8. Há aplicativos próprios para guardar senha em seu celular, não utilize o bloco de notas para isso.

IV. SEGURANÇA EM GERAL (PARA COMPUTADORES E CELULARES)

1. Tenha um antivírus no celular e no computador e o mantenha atualizado.

2. Mantenha seu sistema operacional e navegadores sempre atualizados.

3. Não compartilhe senhas e tokens com outras pessoas.

4. Utilize senhas complexas nos computadores contas de e-mails.

5. Não abra mensagens de quem não conhece.

6. Evite clicar em links, sejam aqueles enviados por e-mail, sms ou mensagens de whatssApp.

7. Evite colocar seu e-mail principal ou telefone celular principal em bancos de dados abertos tais como OLX ou Webmotors.

8. Habilite o sistema de busca de aparelhos celulares e computadores, ele auxiliará em caso de perda ou subtração. Também permitirá o apagamento remoto salvaguardando seus dados.

9. Tenha Backup físico ou em nuvem.

10. Desconfie sempre de pessoas pedindo dinheiro por qualquer meio. Na dúvida, entre em contato com a pessoa por telefone e certifique-se que é a destinatária do dinheiro e não um golpe.

11. Por fim, faça varredura em *pen drives* e outros dispositivos de armazenamento com frequência com um antivírus. Eles são grandes disseminadores de vírus.

12. Caso você receba telefonema de seu próprio número de telefone, estas situações mostram falhas operacionais das empresas de telefonia móvel; pode se tratar de uma tentativa de golpe; você não conseguirá identificar quem está efetuando a ligação, não tem a opção de retornar a chamada e ainda é onerado. Não atenda esse tipo de ligação. As operadoras não podem se eximir da responsabilidade por falhas na prestação do serviço, alegando desconhecimento. Você deve procurar os órgãos de defesa do consumidor e registrar queixa na Anatel, pois na qualidade de órgão regulador, deverá adotar as medidas cabíveis para solucionar o problema.