REDES SOCIAIS

PRÁTICAS DE SEGURANÇA

PNPC

PROGRAMA NACIONAL
DE PROTEÇÃO DO
CONHECIMENTO SENSÍVEL

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Produção
Departamento de Contrainteligência
Programa Nacional de Proteção do Conhecimento Sensível (PNPC)

Projeto Gráfico
Coordenação-Geral de Relações Institucionais e Comunicação

Impressão
Divisão de Serviços Gráficos

REDES SOCIAIS
PRÁTICAS DE SEGURANÇA

2021

CONTEÚDO

PNPC | PROGRAMA NACIONAL DE PROTEÇÃO DO CONHECIMENTO SENSÍVEL

APRESENTAÇÃO

As redes sociais são um fenômeno relativamente recente na história dos meios de comunicação. Elas ampliam a disponibilidade e o acesso à informação, assim como a capacidade de produzir e disseminar conteúdo. Com essas mídias, cada indivíduo é potencialmente produtor e canal de distribuição de informações.

Ao mesmo tempo em que trazem inovação, as redes sociais e o próprio comportamento dos usuários geram vulnerabilidades que são exploradas por agentes adversos, como hackers, serviços de inteligência e empresas concorrentes. Esses atores podem realizar ações de engenharia social: método usado para enganar, manipular ou explorar a confiança das pessoas. Nesse sentido, há implicações significativas não só para segurança dos indivíduos, mas também de instituições e mesmo de Estados Nacionais. Por isso, é preciso adotar medidas de proteção.

Esta cartilha foi elaborada pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), desenvolvido pela Agência Brasileira de Inteligência (ABIN). Criado em 1997, o PNPC é uma assessoria de segurança que busca promover uma cultura de proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas, com foco na prevenção de ameaças como espionagem, sabotagem e vazamento de informações.

PNPC
PROTEGER COM INTELIGÊNCIA

1

USO DAS REDES SOCIAIS PARA OBTENÇÃO DE INFORMAÇÕES

Ataques que visam obter informações sensíveis possuem três principais fases: a escolha dos alvos, a coleta de informações sobre esses alvos e o ataque propriamente dito. As redes sociais podem ser utilizadas nas três fases de forma mais econômica e menos arriscada do que outros métodos.

1ª Fase: Escolha dos alvos

Se um agente adverso necessita de alguma informação sensível, ele precisa descobrir quem tem acesso a ela para conseguir obtê-la. Em pouco tempo de pesquisa em redes sociais, é possível ter uma lista extensa de possíveis alvos com acesso.

No caso de informações institucionais, a rede profissional LinkedIn é especialmente útil, pois permite que se descubra o nome de várias pessoas que trabalham em um determinado setor de uma organização. Se um concorrente quer ter acesso a informações financeiras de uma empresa, uma pesquisa simples pode retornar uma lista de funcionários do setor, de diretores a estagiários.

Se um hacker precisa de alguém com acesso privilegiado ao sistema de informações de uma instituição, pode buscar os nomes de administradores de sistema, chefes de segurança da informação etc.

2ª Fase:
Coleta de Informações

Na maioria das vezes, um agente adverso consegue reunir informações sobre seus alvos nas redes sociais sem maiores dificuldades, já que são postadas **voluntariamente** por eles.

Por um lado, pode-se encontrar uma série de **dados brutos** sobre os alvos: nome completo, número de documentos, data de nascimento, endereços, contatos, nomes de familiares e outros. Essas informações podem ser utilizadas diretamente, para realizar uma fraude, por exemplo, ou para ajudar a descobrir uma senha, já que as pessoas costumam utilizar parte dessas informações em seus códigos de acesso.

Informações profissionais são especialmente importantes para o planejamento de uma ação pelo agente adverso. É comum que as pessoas publiquem em seus perfis do LinkedIn as datas que começaram a trabalhar em um lugar, quando frequentaram uma universidade, em que cidade etc. Essas informações podem ser utilizadas em uma ação de engenharia social.

No LinkedIn, também é possível obter **detalhes técnicos da infraestrutura** de uma organização. Na experiência postada por um funcionário, pode constar a implementação de um sistema específico e, na área de recomendações e habilidades, a pessoa pode especificar um software em uso na instituição e ser recomendado por um colega que também trabalha no local. Com isso, um hacker pode buscar vulnerabilidades específicas desses sistemas para atacar.

Outro tipo de informação que muitas vezes é esquecida pelos usuários e pode ser muito útil a agentes adversos são os **dados geográficos** vinculados a uma postagem. Há alguns anos, a maioria das redes sociais possibilitava que imagens fossem postadas com seus metadados, informações como data em que foram realizadas, abertura e velocidade de exposição, por exemplo, além dos dados de geolocalização. Como a maioria das pessoas não desabilitava o georreferenciamento das câmeras dos celulares, era muito comum que os usuários nem ao menos soubessem que estavam divulgando sua localização.

Atualmente, boa parte das redes sociais retira os metadados das imagens postadas, mas permitem que uma localização seja inserida por meio do aplicativo relacionado a ela. O Instagram, por exemplo, possui esse recurso, o que é chamado de ***geotagging***.

Isso pode permitir saber onde o alvo se encontra em um determinado momento ou quais locais frequenta. Outra forma de obter essas informações é quando se faz check-in em um estabelecimento utilizando uma rede social, como o Facebook, para poder utilizar a rede wi-fi do local. Essas informações podem ser muito úteis para um engenheiro social na hora de planejar um ataque.

Por outro lado, é possível coletar uma série de **informações de entrelinhas:** quais os interesses, as motivações, os sonhos, as frustrações, as raivas e outros fatores psicológicos da pessoa? Isso é importante para que o agente adverso consiga selecionar uma abordagem mais eficaz para aquele alvo específico.

Do ponto de vista do engenheiro social, a alguém que demonstra um grande apego a bens materiais e a um padrão de vida mais alto, talvez seja mais adequado um oferecimento de recompensa financeira em troca de uma informação do que a quem se mostra ambicioso academicamente, mas sem pretensões financeiras. Para este, convites para eventos e publicações conjuntas talvez proporcionem melhores resultados.

Saber se alguém está insatisfeito com seu emprego ou passando por problemas financeiros também pode facilitar na definição de uma abordagem em detrimento de outra.

Até mesmo questões que podem parecer banais, como hobbies e outros interesses pontuais podem ajudar em um ataque cibernético. Afinal, o alvo é muito mais propenso a abrir um e-mail e a clicar em seu anexo caso tenha interesse em seu assunto.

3ª Fase: Ataque

Tendo as informações colhidas nas fases anteriores, o agente adverso decide como atacar sua vítima. As próprias redes sociais atualmente têm sido vetor dos ataques. Além de permitir interações entre os participantes, elas possibilitam a criação de perfis falsos, chamados de **fantoches**, o que proporciona uma camada de segurança para o atacante ao desvincular a sua identidade real da identidade utilizada no ataque.

Criação de Fantoches

A criação de um perfil em uma rede social é algo extremamente simples. Não é necessário provar sua identidade. Não se pode ter certeza de que um perfil pertence à pessoa que diz ser a proprietária. Por isso, a criação de um fantoche é a primeira ação a ser feita para um ataque.

Na maioria dos casos, são criados **fantoches efêmeros**, feitos para durarem apenas durante aquela campanha específica. Não se investe significativamente no desenvolvimento do "personagem". Apenas informações básicas e algumas conexões são adicionadas para garantir o mínimo de veracidade.

Esse tipo de fantoche costuma ser identificado facilmente, já que tem poucos "amigos", interações e referências. Uma busca simples pela foto do perfil pode revelar imagens tiradas de outras pessoas e até de bancos de imagens.

Apesar disso, os fantoches efêmeros são eficazes, principalmente no LinkedIn, uma vez que muitas pessoas aceitam pedidos de conexão independentemente de conhecer os interlocutores na vida real. Se já houver um contato em comum, a probabilidade de se aceitar uma conexão é ainda maior.

Em alguns casos, é criado um **fantoche persistente**, que é reutilizado em diversos ataques. Nestas situações, notar que o perfil é falso é mais difícil, já que possui uma rede de conexões maior, formada por outros

fantoches e por pessoas reais. O "personagem" é mais bem elaborado: tem currículo acadêmico compatível, histórico profissional, interage com outras pessoas e pode até demonstrar conhecimento de uma área específica.

Fantoches persistentes são difíceis de serem descobertos apenas lendo o perfil. Uma forma de se conseguir detectá-los é cruzando as informações fornecidas com fontes externas às redes sociais, que são mais difíceis de serem manipuladas. Há registros em entidades profissionais? A pessoa já deu alguma entrevista? A imagem dela pode ser comparada com outra fonte? Tudo isso demanda algum trabalho e na maioria das vezes não é feito, o que torna esse tipo de perfil tão eficiente.

Recrutamento

Uma das formas de utilização desses fantoches é no **recrutamento** de pessoas que são identificadas como tendo acesso a informações sensíveis. Como no caso de recrutamentos presenciais, o processo normalmente ocorre gradativamente.

Após a conexão inicial, o agente adverso pode começar uma “amizade” por meio de troca de mensagens. Depois dessa aproximação, pode haver um **convite** para alguma parceria, seja profissional ou acadêmica, como palestrar em um evento, escrever um artigo em conjunto etc.

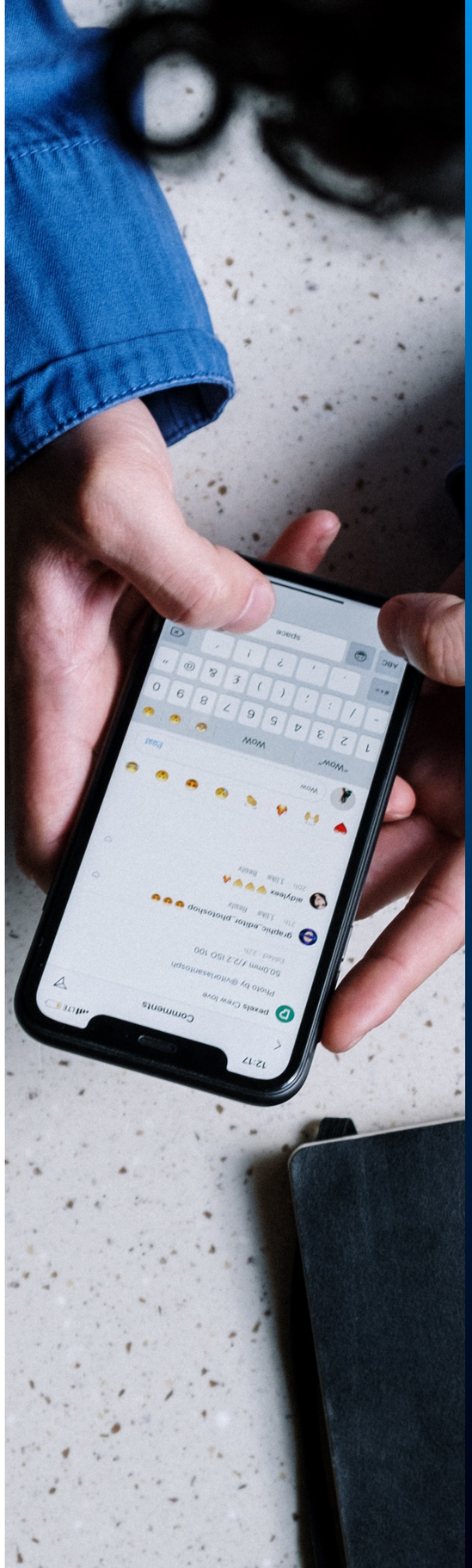
Com o transcorrer deste relacionamento, alguns pequenos pedidos de informação podem começar a acontecer. Então, eles serão gradativamente ampliados para pedidos maiores, que envolvam informações sensíveis.

Entrevista para obtenção de informações

Mesmo que um recrutamento completo não ocorra, um agente adverso pode aproveitar o desenvolvimento de um relacionamento nas redes sociais para conseguir informações.

Alguém pode se passar por funcionário de recursos humanos de uma empresa e tentar extrair informações sobre um concorrente enquanto questiona a experiência de um candidato a uma vaga falsa de emprego. Aplicativos de relacionamento também podem ser utilizados com esse propósito.

Essa técnica é chamada de **entrevista**. Para a Atividade de Inteligência, a entrevista é uma conversa com propósito definido, planejada e controlada pelo entrevistador. Ela pode ser realizada para obter, confirmar ou fornecer dados ou ainda modificar o comportamento de outra pessoa.



Vetor para malwares

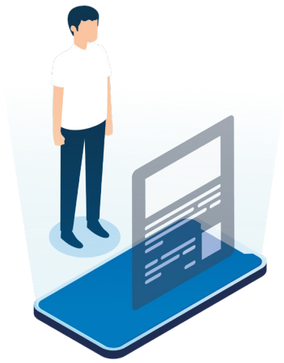
As redes sociais eram utilizadas normalmente nos preparativos dos ataques virtuais, ficando o envio de malwares por conta de e-mails ou links maliciosos. Atualmente, entretanto, até essa fase dos ataques pode ser realizada por meio de mensagens privadas relacionadas às redes.

Outra forma é por meio de links que direcionam o usuário a páginas maliciosas controladas pelo agente adverso. Descobrir se o destino de um link é legítimo ou não é mais difícil em algumas redes sociais, como o Twitter, que utilizam encurtadores de endereço. Assim, tenha sempre cuidado ao clicar em links.

PNPC
PROTEGER COM INTELIGÊNCIA

2

VAZAMENTOS INVOLUNTÁRIOS

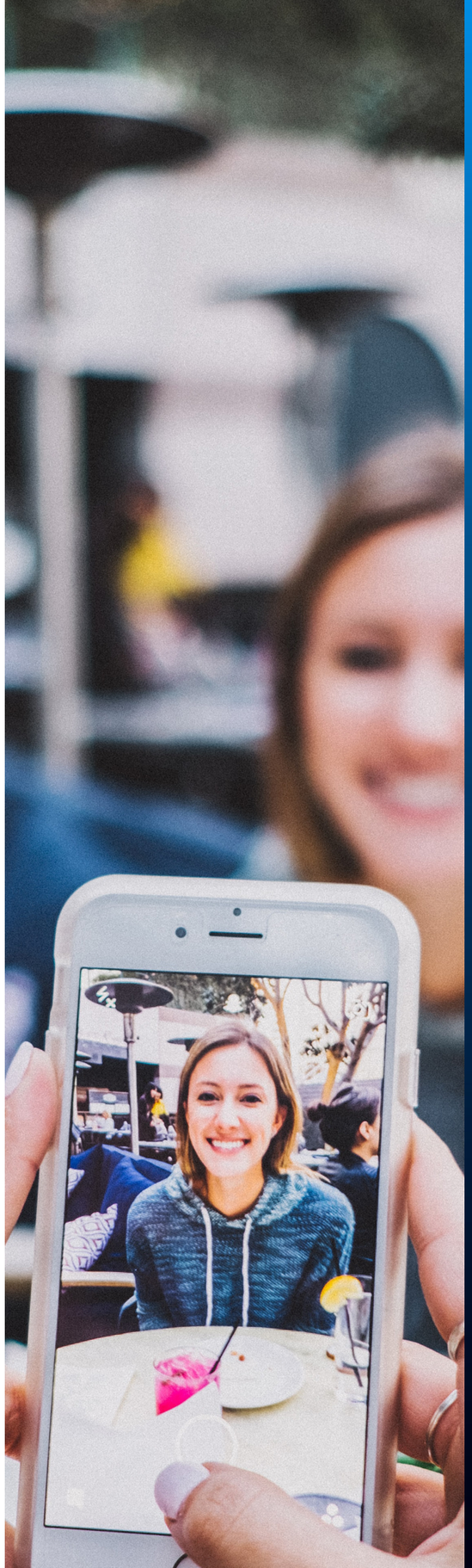


Muitas vezes não é necessário que alguém tome a iniciativa de atacar para que as pessoas tenham problemas com informações sensíveis em redes sociais. Por fazer uso de tecnologias que dependem de interação humana, as redes sociais facilitam a ocorrência de vazamentos involuntários. Quem nunca se confundiu e enviou uma mensagem para o grupo de WhatsApp errado ou publicou algo que não pretendia?

Com a utilização de um **mesmo equipamento para atividades profissionais e pessoais**, é possível que informações profissionais sejam postadas por engano, por exemplo.

Outro facilitador de vazamentos em redes sociais é o fato de que muitas vezes as pessoas não se atentam que **imagens** também têm informações. Dificilmente alguém escreveria o seu número de cartão de crédito em uma rede social. Entretanto, são comuns os casos de fotografias em que estes números podem ser lidos com facilidade. O mesmo acontece com documentos, endereços residenciais e outras informações que as pessoas normalmente hesitariam em publicar.

Às vezes, as informações não estão em primeiro plano nas imagens. Há casos de funcionários fotografados em seu ambiente de trabalho com senhas anotadas em papéis colados em monitores (o que também não é recomendado), que podem ser vistos em segundo plano. Antes de publicar uma foto, procure varrer a imagem para identificar informações que você não gostaria que aparecessem publicamente.



Institucionalmente, é importante que visitantes, funcionários e demais pessoas que tenham acesso às instalações do órgão recebam instruções do que pode e do que não pode fotografar. Dificilmente alguém saberá a classificação de sensibilidade de tudo o que há em um local.

Não sabendo que uma informação é sensível, um funcionário pode publicá-la em sua rede social sem se atentar a eventuais consequências negativas para o órgão. É mais simples controlar a proibição de fotografias dentro de uma instituição do que controlar a proibição de postagens em redes sociais.

Fóruns, grupos de Facebook e outras redes que permitem **debates** sobre temas específicos também são meios que facilitam vazamentos involuntários de informações. Pessoas que participam de discussões em fóruns normalmente são muito interessadas no assunto e, mesmo que inconscientemente, procuram passar uma imagem de especialistas. Um tópico pode começar discutindo algo não classificado, mas o aprofundamento se dar de forma tão gradual que alguém pode passar a fornecer informações sensíveis sem perceber.

PNPC
PROTEGER COM INTELIGÊNCIA

3

PREVENÇÃO

Política Pessoal

O primeiro passo na prevenção de várias ameaças relatadas nesta cartilha, como espionagem e vazamento de informações, é definir uma política pessoal de uso das redes sociais. O que se pretende com aquela rede social específica? Pretende-se ganhar dinheiro sendo um influencer ou apenas entrar em contato com amigos? Isso vai determinar o quanto aquela rede social específica precisa ser aberta ou poderá ser fechada.

Quanto mais riscos se está disposto a assumir, mais aberta ficará a rede social. Há uma relação direta entre a **exposição** de uma pessoa nas redes sociais e os riscos relacionados. Essa exposição se dá tanto pela quantidade de pessoas que podem ver o perfil, ou seja, o quanto ela é aberta, quanto pela quantidade e tipo de informações que são postadas.

Se alguém pretende ganhar dinheiro com o seu perfil no Instagram, precisa que muitas pessoas o vejam. Não faria sentido ter um perfil fechado. Mas pode-se controlar o tipo de informações que são postadas para evitar impactos indesejados. Por outro lado, alguém pode definir que o objetivo de seu perfil é ver o que se passa com seus amigos e mostrar um pouco de sua vida. Dessa forma, pode-se ter um perfil fechado apenas para amigos e aceitar conexões somente de pessoas que conhece na vida real.

Configurações de privacidade e segurança

Tendo tomado a decisão sobre a política pessoal de uso de redes sociais de forma consciente, a próxima etapa é acertar as configurações de privacidade e segurança. Todas as redes sociais possuem áreas específicas onde é possível controlar quem pode ver o que é publicado, quais informações são públicas, quais não são, e assim por diante.

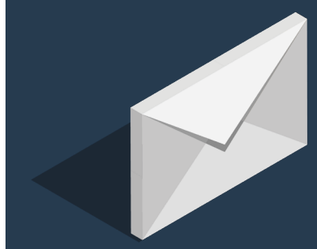
Ainda dentro das configurações de segurança é importante adicionar a opção de duplo fator de autenticação, em que, em determinadas condições, além da senha, é necessária outra comprovação de sua identidade para acessar a rede. Normalmente, essa comprovação é feita por meio de um código enviado para o celular ou e-mail da pessoa.

Compartimentação de perfis

O cruzamento de informações de todos os seus perfis de redes sociais é algo simples de ser feito, principalmente se é utilizado o mesmo nome, e-mail e telefone para registro. Para diminuir seu risco, procure segmentar e compartimentar seus perfis de forma que seja mais complicado ligar um ao outro. Você pode usar nomes e apelidos diferentes em cada rede, por exemplo, e não estabelecer um link direto entre as contas, algo que é possível de ser ajustado nas configurações. Também é recomendável usar diferentes fotos de capa.

Algumas pessoas podem escolher ter perfis públicos para divulgar algo. Nesses casos, pode-se estabelecer dois perfis dentro da mesma rede social: um aberto a todos, para divulgação do que se pretende, e outro fechado, para contato com amigos e familiares. Dessa forma, pode-se publicar assuntos mais pessoais no privado, sem que sejam vistos por todos. Novamente, é importante configurar cada perfil para atender a essa decisão.

Independentemente do número de pessoas que pode acessar o seu perfil, lembre-se de que elas podem compartilhar o seu conteúdo. Certifique-se de que uma imagem não possui informações que você não pretende que sejam divulgadas. Só poste algo que você não se importaria que saísse na capa de um jornal. Afinal, você não sabe quando algo pode viralizar.



Caso acredite que sua instituição foi vítima de ação de espionagem por meio de redes sociais, avise o setor de segurança da sua instituição. Você também pode enviar um e-mail para *reporte@abin.gov.br* para estabelecer contato com a ABIN e relatar o caso.

PNPC

PROTEGER COM INTELIGÊNCIA

PNPC@ABIN.GOV.BR

WWW.GOV.BR/ABIN/PNPC