DOBRA

ARTICLE 19

smartphones & celulares

Hoje em dia utilizamos nossos celulares para todo tipo de atividade, de modo que esses aparelhos estão profundamente integrados em quase todos os aspectos da nossa vida. Isso faz com que os celulares sejam alvos preferenciais quando alguém quer atacar ou acessar informações relevantes sobre você, sua organização ou pessoas com que você mantém relações próximas. Para além de ser um alvo estratégico, de modo geral esses aparelhos são bastante vulneráveis a ataques, sendo que acessá-los ou até assumir o controle das funções do aparelho é uma ação relativamente simples e de custo baixo.

REDE DE TELEFONIA

Assim como os celulares de poucos recursos de hardware (os mais antigos, sem internet), os smartphones geralmente estão conectados a uma rede de telefonia (aquela da sua operadora). E o que isso pode acarretar ao usuário?

LOCALIZAÇÃO FÍSICA DO DISPOSITIVO: por conta da infraestrutura da telefonia é possível a geolocalização dos aparelhos por conta da conectividade com as torres das empresas que fornecem o serviço. Portanto, mesmo com seu GPS desligado é possível saber sua localização e em áreas de maior densidade, onde há maior presença de torres, a localização pode ser mais precisa.

GRAMPO DAS LIGAÇÕES: a forma mais usada para grampear ligações legalmente é utilizando a rede da operadora de telefonia. Ainda que para que um grampo seja feito legalmente pela polícia existam uma série de restrições legais (inclusive a necessidade de autorização judicial), sabemos que essas restrições e a legislação vigente é usada de maneira completamente abusiva na prática. Além de grampos legais abusivos, também são feitos grampos ilegais dessa mesma forma. Por fim, ainda é possível interceptar ligações pela torre telefônica da operadora.

APLICATIVOS E OUTRAS FORMAS DE INTERCEPTAÇÃO

MONITORAMENTO DAS ATIVIDADES E ACESSO A ARQUIVOS DO CELULAR: Outro fator importante nos smartphones é a possibilidade de instalação dos aplicativos e, com isso, permitir o acesso a diversos recursos dos aparelho. Por exemplo, ao instalar o WhatsApp você precisa ceder determinados privilégios para que consiga utilizar satisfatoriamente o aplicativo. Nesse exemplo é possível que o aplicativo acesse recursos como:

FOTOS/MÍDIAS/ARQUIVOS, armazenamento, lista de contatos, câmeras, microfone, informações do Wifi, NFC, Bluetooth, localização (por GPS, WIFI e antenas de telefonia), SMS, contas vinculadas, configurações do sistema etc. São praticamente todos recursos do smartphone disponíveis para o aplicativo. Recursos que nem sempre o usuário comum acessa.

GRAMPO AMBIENTAL MÓVEL?

Seja por meio de aplicativos instalados, seja por meio de outros arquivos maliciosos (vírus) instalados nos seu aparelho, é possível tomar o controle do equipamento de suas funções, inclusive ativando microfones e câmeras para gravar tudo em acontece em seu entorno sem que você perceba.

ATUALIZAÇÕES DE SEGURANÇA

Por fim, outra grande preocupação são os smartphones que acabam passando por um processo de obsolescência programada, onde os recursos de hardware (o equipamento em si) não são compatíveis com os recursos de software (os programas que fazem ele funcionar de determinada maneira). Isso faz com que a falta de atualizações de segurança deixe os celulares vulneráveis a ataques de softwares espiões que conseguem coletar todas informações contidas no aparelho ou mesmo ativar recursos como sua câmera e microfone.

DICAS

_Mantenha sempre seu aparelho atualizado. Atualizações de segurança do Sistema Operacional e de aplicativos devem ser feitas sempre que disponíveis!

_Evite instalar aplicativos desnecessários e que solicitem acesso a recursos do aparelho de maneira desnecessária ao seu funcionamento. Quanto menos aplicativos instalados, melhor!

_Ao instalar um aplicativo, leia sobre as permissões requeridas para ter uma noção do que cada aplicativo pode acessar de seu celular.

_De preferência a aplicativos que disponibilizem o código-fonte (software livre), pois assim é possível que passem por auditorias de segurança e recebam atualizações constantemente.

_Criptografe seu celular!

_Não armazene informações sensíveis no aparelho e não faça conversas sensíveis pelo telefone celular. Se precisar fazer uma conversa mais sensível pelo aparelho, utilize a chamada do Signal (aplicativo de mensagem semelhante ao Whatsapp). A chamada é criptografa e não usa a rede de telefonia, mas a rede de dados (internet).

_Em reuniões sensíveis, não permita a presença de aparelhos celulares na mesma sala, mantendo em outro local.

DOBRA

ARTICLE 19

mídias sociais

A plataforma de mídia social mais acessada do mundo, o Facebook, tem como um dos seus principais lemas "é gratuito e sempre será". Mas como então uma empresa consegue faturar bilhões de dólares sem cobrar por nenhum centavo por acesso dos usuários? A resposta para essa pergunta pode ser a chave para entender porque essas redes sociais precisam que os usuários passem mais e mais tempo em suas plataformas de interação.

TUDO PELA INFORMAÇÃO

Toda interação realizada dentro dessas redes sociais ficam disponíveis, a partir do momento que você aceita os termos de uso, para que as empresas por trás possam criar anúncios dirigidos que são o motor de seus lucros. O conteúdo gerado torna-se muito valioso para empresas criarem perfis de consumo em que as propagandas atingem de maneira certeira seu alvo, ou seja, você! Mas até ai, pode ser criar um perfil de consumo possa até te ajudar a encontrar aquele produto que você estava procurando. Mas, e quando até esses limites são ultrapassados?

CAMPANHAS POLÍTICAS

Casos recentes mostram que até mesmo decisões políticas são capazes de serem influenciadas com anúncios dirigidos a determinados públicos. Talvez você já tenha ouvido falar do caso da empresa Cambridge Analytica que teve acesso a informações vazadas de mais de 50 milhões de perfis de usuários da plataforma. Esses dados serviram para criar um perfil psicológico dos usuários a fim de influenciar na campanha de Donald Trump à presidência dos Estados Unidos. Além do caso Cambridge Analytica houve também a incidência de propagandas russas que disseminavam informações falsas sobre a candidata democrata Hillary Clinton, incluindo acusações de relação da candidata com atentados terroristas cometidos pelo grupo Estado Islâmico.

ACORDOS COM GOVERNOS

Edward Snowden, um ex-funcionário da NSA (Agência Nacional de Vigilância) revelou que o Governo dos Estados Unidos mantinha um acordo secreto com as maiores empresas de tecnologia que fornecem serviço na rede, para que pudessem acessar informações pessoais dos usuários dessas redes, conhecido como programa de vigilância PRISM. As empresas Microsoft, Google, Facebook, Yahoo!, Apple, YouTube, AOL, Paltalk e Skype negaram acordo com o governo, mas as revelações de Snowden mostraram que todo conteúdo dos usuários dessas redes, como logins, senhas, conteúdos de e-mails, transferência de arquivos, fotos, vídeos etc, eram acessados e filtrados pela NSA, que afirma ter acesso direto aos servidores dessas empresas.

CUIDADO COM INFORMAÇÕES PÚBLICAS

No caso do Brasil a condenação das 23 ativistas do Rio foi emblemática sobre aquilo que se publica e as redes de interações dos usuários. Parte fundamental do processo que culminou na condenação por associação criminosa foram informações levantadas pela chamada "ronda virtual". Policiais analisavam as interações entre esses ativistas, como curtidas, compartilhamentos, comentários, identificação em fotos etc. Essa informações depois foram instrumentalizadas para o indiciamento e posterior criminalização dessas ativistas

CONTEÚDO PARA AMIGOS

Configure suas contas para que todo conteúdo seja visível apenas para contatos amigos. Contas abertas e com informações acessíveis por qualquer pessoa podem ter suas fotos, vídeos, publicações, informações pessoais vazadas e utilizadas contra o próprio usuário. Há muitos casos de ataques haters que utilizam dessas informações pessoais para criar situações constrangedoras ou mesmo de risco à integridade física da pessoa.

QUAL OBJETIVO

Ao fazer uma publicação, pense se ela pode trazer risco a você ou ao seu círculo de amizades. Você pode tentar esquecer, mas uma vez publicada a informação ficará para sempre na internet. Nem tudo é publicável!

PESQUISE A FONTE

Informações falsas são largamente utilizadas em contextos políticos. Verifique sempre a fonte de uma informação antes de repassá-la. A difusão de discursos que incitam ódio e medo já levaram a casos como em Myaman, onde o Facebook foi a plataforma de campanha militar contra uma minoria muçulmana que passa por um processo de genocídio.

DICAS

_Remova contatos desconhecidos e/ou suspeitos das suas redes de amizade.

_Remova os aplicativos que podem acessar suas informações pessoais e utilizar seu perfil. No Facebook (Configurações > Aplicativos e Sites > Selecione o aplicativo e > Remover)

_Desconecte sua conta da rede social de outros dispositivos. No Facebook (Configurações > Segurança > "Onde você está conectado" > Editar > Selecione a sessão ativa > Encerrar)

_Troque sua senha com frequência. Use uma senha forte e única para o serviço.

_Gerencie que pode ver cada publicação que você faz. É possível criar grupos entre os seus amigos e escolher para qual grupo cada publicação vai ficar visível quando for postada.

_Nem tudo é publicável. Pense no impacto que uma publicação pode ter se for acessada por adversários e avalie se algumas publicações de conteúdo mais sensível devem mesmo ser feitas pela plataforma.

_Não utilize a sua conta da rede social para acessar serviços em outros sites. Crie sempre um login para cada serviço e nunca utilize a mesma senha para serviços distinto.

DOBRA

O Signal é um aplicativo para troca de mensagens instantâneas de texto, áudio, vídeo e arquivos, com criptografia de ponta-a-ponta, com funcionamento similar ao WhatsApp. Porém, podemos encontrar algumas diferenças que colocam o Signal em um campo da segurança da informação superior ao seu concorrente Whatsapp. E, embora compartilhem do mesmo protocolo de segurança, desenvolvido pela Open Whisper Systems, o Signal disponibiliza seu código fonte (software livre) para que possa ser auditado, onde especialistas independentes de segurança podem contribuir com melhorias significativos ao aplicativo ou mesmo encontrar falhas para que sejam logo corrigidas.

ARTICLE 19

signal

MENSAGEIRO PRIVADO

WHATSAPP, POR QUE NÃO?

No caso do WhatsApp, que possui seu código fonte em segredo (software proprietário), é preciso ter uma confiança política na empresa dona do aplicativo (Facebook) de que dentro do código-fonte não há uma falha de segurança ou mesmo um software intencionalmente instalado (backdoor) que comprometa toda a criptografia.

Se você confia que o Facebook, que lucra bilhões de dólares com coleta e tratamento de dados de seus usuários, não tem interesse em sua localização, agenda de contatos, informações pessoais e toda sua interação com uma rede de pessoas, talvez o WhatsApp seja um bom aplicativo para se utilizar. No entanto, sabemos que a empresa tem como plano de negócios fazer extamente o oposto.

Além disso, ao realizar o backup dos dados do WhatsApp em plataformas como do Google ou iCloud (configuração padrão) todas as informações ficam disponíveis para as respectivas empresas de maneira não criptografada, ou seja, todo conteúdo que foi criptografado entre os usuários é revelado.

SIGNAL, A ALTERNATIVA!

Já o Signal é mantido por uma fundação que não possui o interesse na coleta de dados de seus usuários, registrando o mínimo de informação possível para seu funcionamento. E todas informações entre os usuários e servidores do Signal também são mantidas em segredo (criptografados).

LEMBRE-SE DE ESQUECER

Outro recurso interessante do Signal são as mensagens temporárias, onde o usuário pode configurar o tempo que uma mensagem fica disponível até que seja apagada automaticamente. Isso pode evitar que suas conversas sejam inteiramente lidas caso alguém tenha acesso ao seu aparelho e ele esteja desbloqueado. Ainda sim, encorajamos os usuários a apagarem manualmente os conteúdos de chats que não estejam configurados com mensagens temporárias além de conteúdos sensíveis.

SAIBA QUEM ESTÁ DO OUTRO LADO

No Signal também é possível fazer a verificação de contatos através do Código QR, que deve ser feita pessoalmente. Ao escanear o código de um contato, o número dessa pessoa fica marcado como "verificado". Caso alguém tente se passar por essa pessoa (clonagem do aparelho, por exemplo) você receberá uma mensagem informando que seu código de segurança com aquele contato foi modificado. Se o contato verificado fizer a reinstalação do aplicativo você também receberá essa mensagem. Embora o contato esteja verificado, não é possível saber quem está operando o dispositivo naquele momento.

BLOQUEIE A INSTALAÇÃO DO SIGNAL

Uma maneira simples que pode evitar a clonagem de seu aplicativo é configurar o Bloqueio de Registro com Código PIN. Com ele o aplicativo só poderá ser instalado após uma senha numérica de 4 dígitos que o próprio usuário configura (Configurações -> Privacidade -> PIN de Desbloqueio de Cadastro). De tempos em tempos o Signal te solicita o código para verificação.

DICAS

_Mantenha seu aplicativo atualizado, seja WhatsApp ou Signal ou qualquer outro.

_Caso alguém entre em contato pelo WhatsApp e você não sinta segurança no aplicativo, peça para o contato instalar o Signal e assim prosseguir a conversa.

_Ligações pelo Signal são criptografadas e utilizam a rede de dados. Fazer ligações pelo aplicativo em vez de usar a ligação pela operadora telefônica regular pode ajudar e burlar grampo telefônicos na sua linha.

_Ao receber informações sensíveis pelo Signal, lembre-se de transferí-las para locais mais seguros e não deixa-las armazenadas no celular, que possui outras vulnerabilidades que pode comprometer a segurança dessas informações.

_Caso utilize WhatsApp ative a verificação em duas etapas para evitar que o aplicativo seja instalado em outro dispositivo sem sua permissão.

_Verifique se não há nenhuma sessão ativa do WhatsApp Web. (Configurações > WhatsApp Web > Sair de Todos os Computadores).

DOBRA

ARTICLE 19

senhas

Senhas são a primeira e, geralmente, a única barreira de segurança entre o usuário e um serviço. De tempos em tempos são publicadas as listas com as senhas mais utilizadas e a simplicidade dessas senhas chega a ser assustadora. Como saber se uma senha é fácil de ser quebrada por outra pessoa? E quais cuidados precisamos ter para não acabar com nossas contas todas comprometidas?

"Assuma que o seu adversário é capaz de um trilhão de palpites por segundo": foi o que disse Edward Snowden em um de seus e-mails a cineastra Laura Poitras, diretora do documentário Citizenfour. Métodos de quebra de senha utilizam dicionários inteiros em busca de senhas com palavras comuns (método da "força bruta).

Cuidado com as informações pessoais: as informações dos usuários publicadas em redes sociais podem facilitar em muito um atacante revelar sua senha. É o chamado método de engenharia social, que por meio de simples pesquisas em redes sociais e outros serviços, conseguem descobrir informações preciosas sobre os usuários, como nome, sobrenome, data de nascimento, membros da família, animais de estimação, telefones, endereços, números de documentos pessoais, informações de trabalho, interesses e gostos pessoais etc.

CRIANDO SENHAS SEGURAS

As senhas mais seguras são as que não seguem um padrão claro, sendo aleatórias e que contenham o maior número possível de caracteres. Evitando que os ataques de força bruta e engenharia social, mesmo aliados, não obtenham êxito.

MÉTODO DO DADO - DICEWARE

O método do dado foi criado em 1995 por Arnold Reinhold e utiliza um dado e uma lista de palavras para construir senhas, ou frases-senhas, mais seguras.

1) É recomendado que sua senha seja formada por pelo menos cinco palavras da lista de palavras (link para a lista a seguir). Recomenda-se também que entre cada palavra seja dado um espaço.

2) Para cada palavra, temos que lançar 5 vezes um dado (ou lançar 5 dados de uma vez). Os dois primeiros referem-se às páginas (no topo de cada página é possível encontrar dois números separados por vírgula). Os próximos 3 lançamentos referem-se ao número da palavra que será escolhida dentro daquela página.

3) Faça esse procedimento cinco vezes para encontrar as cinco palavras da sua senha. A lista de palavras em português pode ser acessada em:

https://github.com/thoughtworks/dadoware/blob/master/livreto/dadoware-lista-2e.pdf

EXEMPLO PARA UMA FRASE-SENHA
composta por 5 palavras

DADOS	PALAVRA
5,4 | 333	pronto
1,6 | 641	cacimba
1,1 | 326	achar
3,5 | 152	ganir
2,6 | 553	ela
Senha	pronto cacimba achar ganir ela

Ao criar uma frase-senha, os espaços aumentam a quantidade de caracteres e também ajudam a separar as letras para facilitar a digitação.

Mesmo tendo posse da lista de palavras, o método de força bruta perde sua vantagem, pois a cada palavra aumenta-se exponencialmente a quantidade de combinações possíveis. Para se ter uma ideia, a quantidade de possibilidades contidas em uma frase-senha composta por 5 palavras dessa lista com 7.776 palavras é na ordem de 3 bilhões x 10^{19}. Os dados ainda garantem que cada palavra seja escolhida pela aleatoriedade evitando assim que os métodos de engenharia social consigam ter efetividade.

DICAS

_Troque periodicamente suas senhas de serviços principais em um período não maior do que 6 meses.

_Nunca utilize a mesma senha para serviços diferentes. Se algum serviço tiver vazamento de dados todas suas outras contas também são comprometidas.

_Em serviços com limitação de caracteres, utilize o máximo possível.

_Você pode mesclar letras maiúsculas com minúsculas para dar mais força a sua frase-senha.

_NUNCA deixe senhas anotadas em post-its, agendas ou locais de fácil acesso. Busque sempre memorizá-las ou então utilize os gerenciadores de senhas, como o KeePass.

_Sua senha é de uso pessoal, não a forneça para ninguém.

_Sempre que possível, opte pela autenticação de 2 fatores.

_Não envie senhas e/ou códigos por canais não seguros, somente por meio criptografado.