Workshop - Introdução à Segurança Digital

> Segurança & Privacidade

Coda-Br
2021

O que é segurança da informação?

ABNT NBR ISO/IEC 17799:2005

“Segurança da informação
é a proteção da informação de vários tipos de ameaças (...)
é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware“

Fonte: http://www.aulasemparedes.com.br/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf

O que é segurança da informação?

ABNT NBR ISO/IEC 17799:2005

segurança da informação
preservação da **confidencialidade**, da **integridade** e da **disponibilidade** da informação; adicionalmente, outras propriedades, tais como **autenticidade**, **responsabilidade**, **não-repúdio** e **confiabilidade**, podem também estar envolvidas

Fonte: http://www.aulasemparedes.com.br/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf

O que é segurança da informação?

- **Confidencialidade:** informação disponível só para pessoas autorizadas
- **Integridade:** garantia de que a informação não foi alterada
- **Autenticidade:** garantia sobre quem emitiu a informação
- **Responsabilidade:** garantia da responsabilização por ações ocorridas na transmissão, armazenamento e processamento da informação
- **Disponibilidade e confiabilidade:** garantia de que a informação está disponível quando necessária
- **Não-repúdio / irretratabilidade:** impedimento às partes da comunicação de negarem que ela ocorreu

O que é privacidade?

Do Direito

“A privacidade (*privacy*) pode ser definida como o direito de estar só ou, talvez mais preciso, **o direito de ser deixado só** (...) que remete à **não interferência pelo Estado na vida do indivíduo** (...) também como o poder de se reivindicar ao Estado a tutela dessa privacidade, protegendo o indivíduo de terceiros.**”**

Fonte: “Direito à privacidade” por Alessandro Hirata, 01/04/2017, em PUC-SP

Dados pessoais

Fonte: Campanha “Seus Dados são Você” por Coalizão de Direitos na Rede

Diferença entre segurança e privacidade

Segurança da Informação :

Proteção contra a ataques cibernéticos e acessos indevidos a sistemas diversos (empresariais, públicos)

Privacidade de dados está diretamente ligada a segurança da informação mas é uma perspectiva mais do usuário, como os dados são utilizados, coletados e armazenados.

Diferença entre segurança e privacidade

Workshop - Introdução à Segurança Digital

> Principais ataques

Coda-Br 2021

Tipos de ataques à segurança

- DDoS
- Doxxing
- Man in the middle (MITM)
- Phishing
- Ransomware
- Spoofing
- BEC e EAC
- etc.

DDoS (Distributed Denial of Service)

Um ataque de negação de serviço é um tipo de ataque cibernético que deixa **um site ou recurso de rede indisponível por causa de uma sobrecarga ou tráfego mal-intencionado**, deixando-o assim inoperante.

DDoS (Distributed Denial of Service)

Como identificar?

- Quantidade suspeita de tráfego originária de um único endereço de IP ou de uma faixa de endereços IP
- Grande tráfego de usuários com o mesmo perfil de comportamento, como tipo de dispositivo, geolocalização ou versão de navegador web
- Aumento inexplicado de solicitações de uma mesma página
- Padrões de tráfego incomuns, como picos em horários inusitados ou padrões que parecem artificiais (por ex., um pico a cada 10 minutos)

Doxxing

Consiste em obter **informações de identificação sobre uma pessoa** (dados pessoais como nome, endereço residencial, local de trabalho, dados financeiros, fotos, etc.) na internet para **divulgá-las ao público sem a permissão** da vítima.

Fonte: "O que é doxxing e por que você deveria se importar com isso" Por Douglas Ciriaco, 04/07/2016 em CanalTech

Doxxing

Tudo sobre Nintendo VER MAIS

Nesta quarta-feira (30), a Nintendo decidiu demitir Alison Rapp, funcionária da unidade norte-americana da companhia, que trabalhava no setor de marketing há pelo menos dois anos e meio. O caso virou notícia porque Alison vinha sofrendo ataques por parte do GamerGate, grupo de gamers que assedia, ofende e ameaça mulheres da indústria dos videogames quando elas tentam criticar o machismo existente no segmento.

Doxxing

Jornalistas do Grupo Globo têm celulares vazados e sofrem ameaças por caso Robinho

Quatro profissionais da emissora carioca sofreram ataques de torcedores do Santos que não concordaram com a cobertura sobre o caso de violência sexual do atacante

Ana Thais precisou desativar o WhatsApp após vazamento (Reprodução/Sportv)

Doxxing >> Exposed

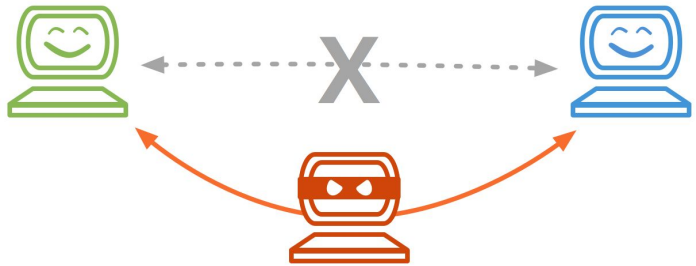
E o que o doxxing tem a ver com Hong Kong?

As práticas de doxxing foram muito difundidas na China em 2019, durante uma série de protestos pró-democracia. As autoridades locais alegam que as atividades foram usadas para divulgar nomes de policiais que repreenderam as manifestações e de funcionários judiciários envolvidos em ações contra ativistas.

China quer evitar novos casos de doxxing em massa. Foto: Jimmy Siu/Shutterstock

Man in the middle (MITM)

O invasor se posiciona entre duas partes que tentam comunicar-se, gozando de uma posição de confiança e interceptando as mensagens enviadas.



Fonte: "O que é um Ataque Man-in-the-Middle?" Por Serge Malenkovich, 10/04/2013, em Karpersky Daily

Man in the middle (MITM)

Por exemplo:

- envio de contas / faturas / boletos falsos
- WiFi aberto

Variante: **man-in-the-browser (MITB)**
O agressor implementa um código malicioso no browser do computador de suas vítimas e o malware silenciosamente grava informações.

Fonte: "O que é um Ataque Man-in-the-Middle?" Por Serge Malenkovich, 10/04/2013, em Karpersky Daily

Phishing

É o crime de enganar as pessoas para que elas **compartilhem suas informações pessoais e/ou confidenciais** como senhas e número de cartões de crédito.

Phishing

Em geral se utiliza de técnicas que **confundem o/a destinatário/a** e, geralmente, usam de expressões e linguagem que dão **sensação de urgência**.

Muitas vezes levam a **links que podem se parecer com o "site original"** esperado e que induzem a passar as informações desejadas.

Phishing
Exemplo

Votre domaine ask-ar.xyz a été expiré

Thursday, December 31, 2020 09:40 -03

paiement.gandi.net

To

ask-ar.xyz

Cher(e) hébergé(e),

Le(s) nom(s) de domaine(s) ci-dessous arriveront à expiré.

Nom de domaine : ask-ar.xyz

En cas de non réglement. Votre nom de domaine sera donc suspendu d'ici quelques minutes.

Pour réactiver le nom de domaine, il vous suffit:

Renouvelez-le dès maintenant.

La facture acquittée vous parviendra sous peu, signalant le renouvellement de votre service pour la période choisie.

Si vous avez besoin d'aide, vous pouvez contacter le support technique.

Merci de votre confiance envers nos services

Cordialement,

GANDI - https://gandi.net

Phishing
Exemplo

```
Return-Path: <security@o3msrl.com>
Delivered-To: diego@ask-ar.xyz
Received: from spool.mail.gandi.net (spool3.mail.gandi.net [217.70.178.212])
        by nmboxes5.sd4.0x35.net (Postfix) with ESMTPS id B375440079
        for <diego@ask-ar.xyz>; Thu, 31 Dec 2020 12:40:55 +0000 (UTC)
Received: from mta50.o3msrl.com (unknown [172.96.114.12])
        by spool.mail.gandi.net (Postfix) with ESMTPS id D6042AC15C4
        for <contato@ask-ar.xyz>; Thu, 31 Dec 2020 12:40:53 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=mail1; d=o3msrl.com;
 h=Content-Type:MIME-Version:Date:Subject:From:Reply-To:Message-ID:
 List-Unsubscribe:List-ID:To;
 bh=X+wpx48JgcCIIS+3IQAxjS+2eBFdCnH1OC4wADDllKM=;
 b=BOxcijjOr3qMsxdTwVRXil6X+SuJKIatyqHZ9E7VruoJiknVMqA+eILIjPkPCWqlzXaJR2WeVqjD
   H9NBrHgAtXN+y61oRyvRfkDALMjG0uty9v6Sg2j7SzsXPkdeEDiZeLw4Jcm5g5S4EIUKxS8thCQP
   Wc4bpQK2GcD0sLOdoic=
Authentication-Results: mta1.o3msrl.com; dkim=none reason="message not signed"
Content-Type: multipart/alternative; boundary="------------080907090709080107070604
MIME-Version: 1.0
Date: Thu, 31 Dec 2020 13:40:29 +0100
Subject: =?utf-8?B?Vm90cmUgZG9tYWluZSBhc2stYXIueHl6IGEgw6l0w6kgZXhwaXLDqQ==?=
From: "paiement.gandi.net" <security@o3msrl.com>
Reply-To: "paiement.gandi.net" <security@o3msrl.com>
X-FBL: 1_121_1139_0_636F6E7461746F4061736B2D61722E78797A
Message-ID: <MTM5OTC2.NDK3NTA5OQ.113911712311340202029147427092l@o3msrl.com>
List-Unsubscribe: <mailto:security@o3msrl.com?subject=Unsubscribe:contato@ask-ar.xy
List-ID: <da3d85634db61b2bdc1756d6e6631ce7.121.localhost>
Precedence: Bulk
To: "ask-ar.xyz" <contato@ask-ar.xyz>
X-GND-Status: LEGIT
```

Phishing
Exemplo

```
Return-Path: <security@o3msrl.com>
Delivered-To: diego@ask-ar.xyz
Received: from spool.mail.gandi.net (spool3.mail.gandi.net [217.70.178.212])
        by nmboxes5.sd4.0x35.net (Postfix) with ESMTPS id B375440079
        for <diego@ask-ar.xyz>; Thu, 31 Dec 2020 12:40:55 +0000 (UTC)
Received: from mta50.o3msrl.com (unknown [172.96.114.12])
        by spool.mail.gandi.net (Postfix) with ESMTPS id D6042AC15C4
        for <contato@ask-ar.xyz>; Thu, 31 Dec 2020 12:40:53 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=mail1; d=o3msrl.com;
 h=Content-Type:MIME-Version:Date:Subject:From:Reply-To:Message-ID:
 List-Unsubscribe:List-ID:To;
 bh=X+wpx48JgcCIIS+3IQAxjS+2eBFdCnH1OC4wADDllKM=;
 b=BOxcijjOr3qMsxdTwVRXil6X+SuJKIatyqHZ9E7VruoJiknVMqA+eILIjPkPCWqlzXaJR2WeVqjD
   H9NBrHgAtXN+y61oRyvRfkDALMjG0uty9v6Sg2j7SzsXPkdeEDiZeLw4Jcm5g5S4EIUKxS8thCQP
   Wc4bpQK2GcD0sLOdoic=
Authentication-Results: mta1.o3msrl.com; dkim=none reason="message not signed"
Content-Type: multipart/alternative; boundary="------------080907090709080107070604
MIME-Version: 1.0
Date: Thu, 31 Dec 2020 13:40:29 +0100
Subject: =?utf-8?B?Vm90cmUgZG9tYWluZSBhc2stYXIueHl6IGEgw6l0w6kgZXhwaXLDqQ==?=
From: "paiement.gandi.net" <security@o3msrl.com>
Reply-To: "paiement.gandi.net" <security@o3msrl.com>
X-FBL: 1_121_1139_0_636F6E7461746F4061736B2D61722E78797A
Message-ID: <MTM5OTC2.NDK3NTA5OQ.1139117123113402020291474270921@o3msrl.com>
List-Unsubscribe: <mailto:security@o3msrl.com?subject=Unsubscribe:contato@ask-ar.xy
List-ID: <da3d85634db61b2bdc1756d6e6631ce7.121.localhost>
Precedence: Bulk
To: "ask-ar.xyz" <contato@ask-ar.xyz>
X-GND-Status: LEGIT
```

Phishing

Como ver o código fonte do email no gmail:

- Abra o e-mail onde está o cabeçalho que você quer verificar.
- Ao lado de Responder ↩, clique em Mais ⋮ > **Mostrar original**.

Se você não usar gmail → ferramenta do Google que ajuda a ler o cabeçalho dos emails:

- Copie o "código da mensagem" (Message Source).
- Abra a ferramenta de cabeçalhos de mensagens.
- Cole o conteúdo em "Colar cabeçalho do e-mail aqui".
- Clique em Analisar o cabeçalho acima.

Referência: https://support.google.com/mail/answer/29436?hl=pt-BR

Workshop - Introdução à Segurança Digital

Phishing

Agora é com vocês:

http://phishingquiz.withgoogle.com/

Ransomware

Trata-se de um cyberataque feito por criminosos que **encriptam os arquivos da vítima e cobram resgate para devolver o acesso**.

Segundo o Internet Threat Security Report (ISTR 2016), em 2015 mais de 1,5 milhões de malwares foram criados por dia, com mais de 430,5 milhões de ocorrências registradas pela Symantec - cerca de 35% a mais do que no ano anterior.

Ransomware

O GLOBO ECONOMIA

BUSCAR ACESSE NO

EXCLUSIVO PARA ASSINANTES

ECONOMIA

Brasil é o principal alvo de hackers que sequestram bancos de dados

Home office em larga escala na pandemia abre mais oportunidades para criminosos invadirem sistemas e pedirem resgate para liberá-los

Sérgio Matsuura, Maurício Ferro e Ivan Martínez-Vargas
06/12/2020 - 04:30 / Atualizado em 07/12/2020 - 19:26

Newsletters

Contágio virtual. Com a pandemia e a massificação do trabalho remoto, criminosos digitais têm agora mais oportunidades para ataques Foto: ALY SONG / REUTERS

Ransomware

O relatório da Kaspersky “Panorama de Ameaças na América Latina” (set/2020) apontou em média 5 mil tentativas de ataque com ransomware por dia, quase metade (46,7%) era contra alvos no Brasil.

— De uma hora para outra, foi todo mundo para o home office. Empresas tiveram que colocar funcionários em trabalho remoto às pressas, e o acesso mais comum foi via RDP, *remote desktop protocol*, que já é nativo do Windows. Acontece que esse protocolo tem falhas, e muitas empresas demoram para instalar as correções — explica. — No Brasil, a média diária de ataques de força bruta contra o RDP era de cerca de 400 mil. Com a pandemia, tivermos picos de 2,5 milhões.

Fonte: “Brasil é o principal alvo de hackers que sequestram bancos de dados” Por Sérgio Matsuura, Maurício Ferro e Ivan Martínez-Vargas, 06/12/2020 em O Globo

Ransomware

READ, HACK, REPEAT
THE HACK
Notícias
Malwares
STJ é vítima de ransomware e tem seus dados e os backups criptografados
Guilherme Petry — há 6 meses
Categorias
Especiais
Denúncias
Sobre
Contato
Entrar
ASSINATURA
Hey, assina a nossa newsletter.

Ransomware

Portal Espera Feliz

Notícias Colunistas Cidade Submersa Autores convidados Prosas da Cidade Contato

Cartório de Espera Feliz tem dados do computador sequestrados

Criminosos cibernéticos criptografaram os arquivos do computador e exigem o equivalente a R$ 12.500,00 para liberação dos dados.

Publicado em 27/05/2016 - 11:45 | Última atualização: 07/06/2017 - 14:33

Um cartório de registro de imóveis de Espera Feliz foi vítima de um "sequestro" dos dados de um dos seus computadores, na última terça-feira (24).

Ransomware

uol
NaTelinha
Televisão
Que situação
Afiliada da Globo sofre ataque hacker e vive dias de pane no sistema
Rede Bahia contratou empresa para recuperação

Ransomware

Quanto?

O resgate varia de acordo com: complexidade do sistema invadido, o tamanho e a importância da corporação.

Resgates variam alguns dólares a milhões de dólares.

São alvos desde usuários domésticos, pequenos e médios empreendedores até grandes corporações, como centros médicos / farmacêuticos.

Ransomware

Como?

A principal forma de entrada no sistema:
phishing de e-mails carregados com a ameaça, (99% dos casos)

Outras formas de entrada: sites maliciosos, apps vulneráveis, links suspeitos em redes sociais e falsos pedidos de atualização de programas.

Ransomware

Será que?!

Se você está conseguindo mexer no seu sistema,
é sinal que ele não foi invadido.

Isso porque **a grande característica do ransomware é justamente bloquear o seu uso**. Para isso, o invasor codifica os dados do usuário em segundo plano, sem que ninguém perceba, e depois de tudo pronto emite um aviso que o sistema está bloqueado e que será necessário o pagamento de um resgate para a liberação de uma chave de segurança restabelecendo o acesso.

Spoofing

O termo vem do verbo em inglês *spoof* (imitar, fingir) que em Tecnologia da Informação é um jargão usado para **falsificação**.

É um tipo de ataque em que **alguém se passa por outra pessoa ou por uma empresa legítima**, no intuito de roubar dados, invadir sistemas e/ou espalhar malwares.

Spoofing

Tipos:

- Spoofing de ID
- Spoofing de DNS
- Spoofing de chamadas e/ou SMS
- Caller ID Spoofing
- Spoofing de e-mail

Fonte: "O que é spoofing?" Por Ronaldo Gogoni em TecnoBlog

Spoofing

Exemplo:

> Whatsapp

Uma conta com um número qualquer é criada usando foto e nome da vítima.
Na sequência, ocorre a busca por contatos da vítima (localizados pelas redes sociais e bases de dados pessoais vazadas). Esses contatos recebem pedidos de ajuda / transferência de dinheiro.

Mais de 5 milhões de brasileiros já foram vítimas de clonagem de WhatsApp em 2020
(em média de mais de 15 mil vítimas do Spoofing por dia no Brasil)
segundo a PSafe

Business Email Compromise (BEC)
Email account compromise (EAC)

BEC e EAC são tipos de fraude por e-mail em que o invasor se apresenta como **alguém em quem o destinatário deve confiar** - normalmente um colega, chefe ou fornecedor.

O remetente pede ao destinatário para **fazer algo que seria indevido um estranho pedir, mas que pelo elo de confiança o destinatário não estranha tanto** (transferência eletrônica, alterar dados bancários para pagamentos futuros e assim por diante).

Fonte: "The Definitive Email Security Strategy Guide" Por ProofPoint

Business Email Compromise (BEC)

Principais tipos, segundo FBI:

- Fraude CEO
- Comprometimento de conta
- Esquema de fatura falsa
- Roubo de identidade de advogado
- Roubo de dados

Business Email Compromise (BEC)

BEC - exemplo:

Remetente: fulano@empresa.com.br
Destinatário: voce@empresa.com.br

Remetente: fulano@empresa.com
Destinatário: voce@empresa.com.br

Email account compromise (EAC)

EAC exemplo:

Remetente: fulano@empresa.com.br
Destinatário: voce@empresa.com.br

O invasor obtém o controle de uma conta de e-mail legítima

Workshop - Introdução à Segurança Digital

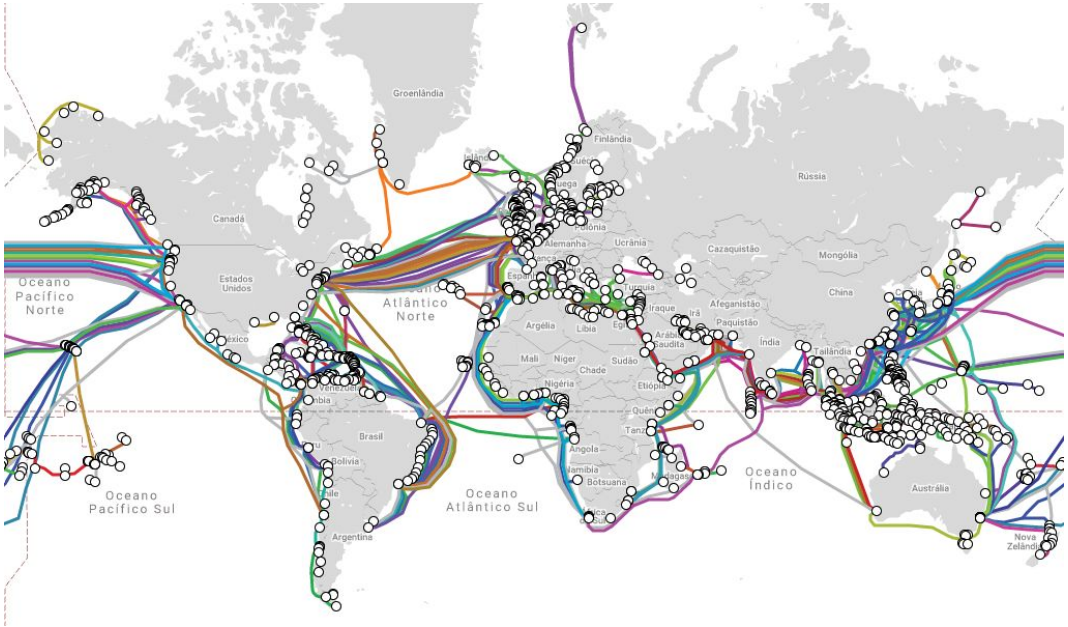
> Infraestrutura

Coda-Br
2021

A nuvem (the cloud)

Fonte: “Conheça um cabo submarino de transmissão de dados” Por Guilherme de Souza, em 12/08/.2013 em HyperScience

A nuvem (the cloud)



Fonte: Submarine Cable Maps

Workshop - Introdução à Segurança Digital

Quantos e quais cabos que servem o Brasil não passam pelos EUA? De qual(is) cidade(s) brasileira(s) parte(m)?

https://www.submarinecablemap.com/

A nuvem (the cloud)

A nuvem (the cloud)

A nuvem (the cloud)

Não existe nuvem (etéreo)
é só o(s) computador(es) de outra pessoa que não você

- O que se chama de “nuvem”: **serviços online** que expandem as capacidades de armazenamento, processamento, etc, de um computador ou celular.
- Apesar de úteis, **é necessário avaliar**: impacto no seu modelo de negócio, riscos, jurisdição, histórico de compromisso com segurança e privacidade, etc.

Backups

É a cópia de dados de um dispositivo de armazenamento em outro

- Podem ser feitos em dispositivos físicos próprios ou de outrem (serviços em nuvem) → categorizar o que convém guardar em nuvem e o que convém guardar somente em dispositivo próprio

- Precisam estar **sempre atualizados** para cumprir sua função de restauração em caso de perda ou comprometimento de dados

Backups

Aspectos a serem considerados:

- Quais informações (categorização)
- Frequência de atualização (por categoria)
- Quantidade de versões a guardar (contexto regulatório)
- Por quanto tempo armazenar a informação (por categoria)
- Quantidade de informação a armazenar (por categoria)
- Segurança
    - Criptografado ou não
    - *Inhouse* ou *outsourced*

Criptografia

A arte de esconder ou proteger informações (Silva, 2019)

-Implementação de Confidencialidade, Integridade, Autenticidade.

Chave Simétrica - a mesma chave é usada no envio e recebimento da mensagem, ou seja, encriptar e decriptar uma mensagem. Somente o remetente e o destinatário devem conhecer a chave secreta, pois esta é a única maneira de obter a confidencialidade.

Chave Assimétrica - Na criptografia assimétrica, cada parte da comunicação possui um par de chaves. Uma chave é utilizada para encriptar e a outra para decriptar uma mensagem. A chave utilizada para encriptar a mensagem é pública, isto é, ela é divulgada para o transmissor; enquanto a chave para decriptar a mensagem é privada, isto é, ela é um segredo pertencente ao receptor.

Workshop - Introdução à Segurança Digital

Desafio prático

Cifra de césar

por Nina da Hora

Workshop - Introdução à Segurança Digital

> Comportamento Seguro

Coda-Br 2021

Comportamento seguro

Segurança

Se o sistema é tão inseguro, por que empresas como Apple investem nessa tecnologia? É um consenso que sistemas de leitura de impressões digitais são fáceis de hackear. Para muitas pessoas, contudo, eles representam um aumento de segurança. Elas usam "senhas fracas", sequências que podem ser facilmente descobertas, como "123456" ou "qwerty" e, por isso, ficam vulneráveis. O aparecimento de dispositivos com leitores de digitais está ligado a isso. Para pessoas que são descuidadas com suas senhas, eles oferecem uma boa saída: são confortáveis e passam a falsa sensação de segurança. Mas, note-se, é uma falsa sensação.

Fonte: "Sistemas biométricos não são seguros como imaginamos, diz especialista", Por Guilherme Pavarin, 01/02/2015, em Veja

Comportamento seguro

Segurança

Para se ter uma ideia, pesquisadores do Instituto de Informática do Japão (NII) realizaram um estudo que afirma que o leitor de digitais de um aparelho pode ser desbloqueado por meio de uma foto. E não precisa ser nada elaborado: uma simples foto fazendo o famosíssimo “V da Vitória” já torna suas digitais amplamente disponíveis.

Mas não se engane achando que isso só acontece com sistemas de reconhecimento por digitais. Recentemente, um pesquisador alemão conseguiu burlar o sistema de reconhecimento por íris do Samsung Galaxy S8 usando apenas uma câmera digital, uma impressora a laser e lentes de contato.

Fonte: ”Biometria em smartphones: o recurso é realmente seguro?“ 31/08/2017 em UOL

Comportamento seguro

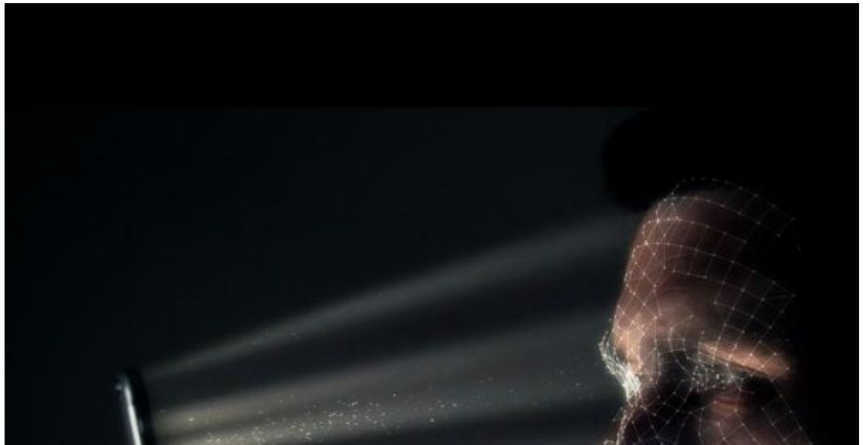
Privacidade

Home > Internet

Empresas que oferecem dados biométricos de brasileiros são alvo de investigação do MP

CertBio, CredDefense e Acesso Digital trabalhariam com um banco de dados de imagens de mais de 70 milhões de brasileiros

Jonas Valente, Agência Brasil
17/08/2018 às 17h18



Comportamento seguro

Privacidade

Em um anúncio relalizado em sua página oficial, o WhatsApp avisou que está liberando o recurso para **proteger o aplicativo via impressão digital** no Android, de forma parecida com o que já ocorria no iPhone graças ao Touch ID e ao Face ID. A nova função, vale lembrar, não bloqueia chamadas, mas dificulta o acesso ao aplicativo após um período de inatividade para que outras pessoas não leiam suas mensagens.

Fonte: "WhatsApp libera bloqueio do aplicativo por impressão digital; veja como fazer" Por Alvaro Scola, editado por Eduardo Nuvens, 13/08/2019, atualizada em 29/09/2021, em Olhar Digital

Comportamento seguro

Privacidade

"Quando o assunto é segurança, dificilmente recomenda-se ignorar uma opção de defesa. Como o WhatsApp agora pode impor um bloqueio por impressão digital no Android, quem busca mais proteção deveria, a princípio, ativá-lo. Mas o recurso tem baixa eficácia e, pior do que isso, pode **criar hábitos que prejudicam a sua segurança** (...) **O bloqueio do telefone jamais deve ser menos rigoroso que a segurança de um aplicativo, porque um app só pode se proteger se a integridade do sistema colaborar** (..) Infelizmente, a ativação do bloqueio no WhatsApp pode nos levar a pensar exatamente dessa forma, priorizando um aplicativo muito usado em detrimento do próprio aparelho. O resultado será um celular bem menos seguro, inclusive para o próprio WhatsApp."

Fonte: "Por que você não deve usar o desbloqueio por impressão digital do WhatsApp" Por Altieres Rohr, 26/11/2019, em Portal G1

Comportamento seguro

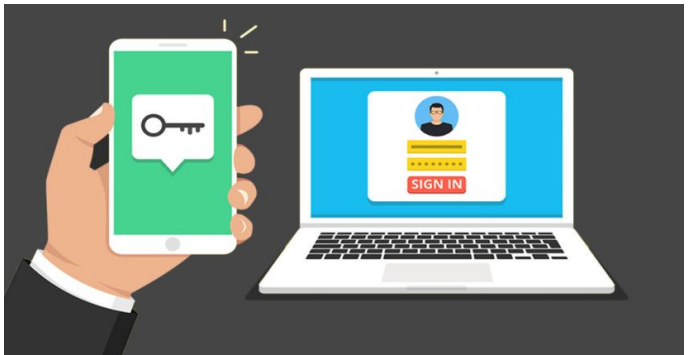
Mapeando as ameaças

- **Acesso aos equipamentos físicos:** na redação, em reportagem, em manutenção...
- **Ameaças judiciais:** ordens de busca e apreensão, acesso a dados em servidores, etc.
- **Utilização de má fé de informações públicas:** *doxxing,* perseguição...
- **Perda ou roubo de equipamento ou dados**
- **Interrupção de serviços essenciais** (nuvem, apps, etc)

Comportamento seguro

No geral, o que fazer:

- Coloque **travas** na tela do seu celular, tablet e notebook
- Configure um **intervalo de tempo** para a trava automática
- Use **senhas fortes** e **duplo fator de autenticação** (2FA)



Comportamento seguro

- **Nunca** abandone seu celular / tablet / computador com a tela desbloqueada

- **Nunca** guarde senhas, informações de cartão de crédito ou outras informações sensíveis em navegadores

- **Sempre** use guias anônimas no navegador quando estiver num dispositivo que não seja o seu

DDoS

Como prevenir:

- rotear para um black hole (rota nula)
  → há risco de perda de tráfego legítimo
- rate limiting (limitação do número de solicitações que um servidor aceitará por um período de tempo)
  → não é eficaz contra DDoS complexos
- firewall de aplicativos web (ferramenta capaz de ajudar a mitigar o ataque de DDoS na camada de aplicação)
  → não é eficaz contra DDoS complexos

Mais dicas aqui: O que é ataque DDoS?

Doxxing

Como prevenir:

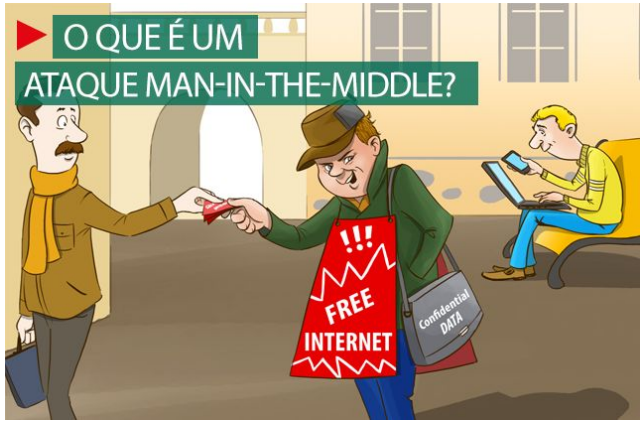
- limitar as informações pessoais disponíveis online
- usar uma VPN (virtual private network) para proteger seu IP
- evitar responder quizzes online (muitas vezes eles perguntam por informações “inofensivas” e mapeiam preferências)
- requerer remoção de informações pessoais do Google (uma pessoa pode requisitar que suas informações saiam dos mecanismos de busca e outras plataformas / redes sociais)

Mais dicas aqui: Protect yourself from "Doxxing"

Man in the middle (MITM)

Como prevenir:

- HTTPS
- evitar usar WiFi abertos/públicos
- só usar redes confiáveis para comunicações críticas
- manter seus sistemas operacionais / programas / softwares atualizados
- manter seu antivírus atualizado



Fonte: "O que é um Ataque Man-in-the-Middle?" Por Serge Malenkovich, 10/04/2013, em Karpersky Daily

Phishing

Como prevenir:

- não clicar em nenhum link sem pensar
- não responder a um email suspeito de phishing
- se o email/mensagem recebido/a é referente a algum serviço que vocês assinam, entrar no site do serviço (sem usar qualquer link do email) e verificar a situação
- não apagar um email de phishing imediatamente → marcar o email como “phishing”

Fonte: “O que é um Ataque Man-in-the-Middle?” Por Serge Malenkovich, 10/04/2013, em Karpersky Daily

Ransomware

Como prevenir:

conter a curiosidade
- evitar clicar em “avisos” que podem conter links maliciosos
- evitar abrir e-mails de desconhecidos e spam em geral
- jamais clicar em links cuja procedência é desconhecida

ser desconfiado
- instalar apenas programas de fontes confiáveis
- desconfiar de links e vídeos enviados por amigues que não têm o perfil de enviar este tipo de conteúdo

ter rotinas / processos seguros
- manter programas atualizados (inclusive antivírus)
- prever varreduras automáticas e periódicas de antivírus
- estar sempre com o backup atualizado e desconectado do computador

Ransomware

O que fazer se for vítima?

- Entre em contato imediatamente com o seu suporte de TI
- Evite pagar o resgate
- Invista na segurança da informação

Para saber mais: **Você foi vítima de um ataque de Ransomware (sequestro de dados)? Saiba o que fazer. Inputec, 2020**

Spoofing

Como prevenir:

- ficar atento(a)
- confirmar por outro meio de comunicação
- verificar sempre antes de clicar em links
- ter cuidado com anexos estranhos
- desconfiar da natureza das solicitações, como sites de bancos que pedem números de RG e CPF, além do básico (número de cartão, senha e código de segurança)

Para saber mais: “O que é spoofing e como posso me proteger dele?” Em AVAST

Spoofing

- usar senhas fortes
- trocar de senhas regularmente
- ativar a verificação em duas etapas (de preferência, não usar o SMS ou o número de telefone como verificador)
- informar as tentativas de spoofing
- usar antivírus (atualizado)
- verificar o DNS do seu roteador e estar sempre atento ao endereço do site suspeito, que em geral difere em detalhes do legítimo (para Spoofing de DNS)

Para saber mais: "O que é spoofing e como posso me proteger dele?" Em AVAST

Business Email Compromise (BEC)
Email account compromise (EAC)

Do que desconfiar:

- executivos de alto nível pedindo informações incomuns
- solicitações para não se comunicar com outras pessoas
- solicitações que ignoram os canais / procedimentos usuais
- mensagens com erros de escrita e formatos de data incomuns
- domínios de e-mail e endereços “Responder a” que não correspondem aos endereços do remetente

Mais dicas aqui: Impostor Email Threats

Nuvem

O que evitar:

- não armazenar dados sensíveis desnecessariamente;
- considerar excluir ou manter apenas uma cópia fora da Internet de dados sensíveis
- usar e-mails descartáveis para cadastros temporários

O que você tem em seu email, redes sociais ou outras plataformas?

Backups

- Sempre tenha uma cópia física que fique com você de arquivos e dados mais sensíveis
- Tenha um HD externo (mas você também pode usar pendrive que guarde em local seguro)
- Tenha uma rotina de backup: fazer uma atualização mensal por exemplo (deixe alarme programado na sua agenda eletrônica)

Senhas

- Não usar senhas óbvias ou fracas
- Não compartilhar senhas com ninguém
- Nunca salvar / guardar senhas e, arquivos comuns, no email, no Docs
- Não usar a mesma senha em mais de um site / ferramenta
- Guardar suas senhas em local seguro
- Trocar periodicamente suas senhas

gerenciador de senhas

Senhas fracas

Como evitar?

- Não usar informações pessoais
  Exemplos: datas de nascimento, aniversário, casamento, falecimento; nomes (próprio, de filho(a)(s), animais, etc.); favoritos (filme, livro, comida, etc.)

- Não usar sequências de números ou letras
  Exemplos: 123456, abcdefg, qwerty, etc.

- Não usar repetições ou espelhamentos
  Exemplos: 11111111, aaaaaaaa, 123321, qwertytrewq, etc.

  Senhas mais utilizadas em 2020:
  123456, 123456789, qwerty, password, 1234567

Senhas fortes

- Busque formas de criar senhas sem sentido ou aleatórias
- Use senhas **longas** (com mais de 12 caracteres)
- Use senhas que não sejam palavras que estão no dicionário
- **Mesclar tipos de caracteres**: letras (MAIÚSCULAS e minúsculas), núm3r0s e esp&c!4i$

Leia mais dicas para criar senhas fortes aqui: Surveillance Self-Defense

Workshop - Introdução à Segurança Digital

> Ferramentas

Coda-Br 2021

Rotina antidoxxing

Ajuste periodicamente suas configurações de privacidade:

Quais detalhes ficam disponíveis para diferentes círculos de amizade?

- Facebook: https://www.facebook.com/help/325807937506242?ref=tos
- Instagram: https://help.instagram.com/196883487377501

Rotina antidoxxing

Excluir seu histórico de navegação periodicamente

No Chrome:

Limpar o histórico

1. No smartphone ou no tablet Android, abra o app Chrome .
2. No canto superior direito, toque em Mais > **Histórico**.
   - Se a barra de endereço estiver na parte inferior da tela, deslize para cima nessa barra. Toque em Histórico .
3. Toque em **Limpar dados de navegação**.
4. Ao lado de "Período", selecione a parte do histórico que você quer excluir. Para limpar tudo, toque em **Todo o período**.
5. Selecione "Histórico de navegação". Desmarque todos os outros dados que você não quer excluir.
6. Toque em **Limpar dados**.

Rotina antidoxxing

Excluir seu histórico em mecanismos de busca periodicamente

No Google:

Gerenciar e excluir o histórico de pesquisa

Quando você pesquisa no Google com a Atividade na Web e de apps ativada, atividades como o histórico de pesquisa são salvas na sua Conta do Google. Nós usamos as atividades salvas nos Serviços do Google para proporcionar experiências mais personalizadas, como recomendações de conteúdo e de apps.

Na página Minha atividade , é possível:

- excluir o histórico de pesquisa salvo na sua Conta do Google;
- gerenciar as configurações de pesquisa, como qual atividade o Google salva e quando ele exclui automaticamente o histórico.

A nuvem (the cloud)

Alternativas ao DropBox, GoogleDrive, iCloud e OneDrive:

- NextCloud
- SpiderOak

Para gerar usar e-mails descartáveis para cadastros temporários:

- https://www.mailinator.com
- https://www.guerrillamail.com/pt/
- https://temp-mail.org/pt/

Backups

Serviços de backup (em nuvem) dos próprios fornecedores:

- WhatsApp para Google Drive
- iPhone e iPad pelo itunes e iCloud
- Windows usando OneDrive

Outros serviços de backup (em nuvem):

Blackblaze, Carbonite, BrasilCloud, iDrive, ElephantDrive, etc.

Backups

Backup Criptografado para WhatsApp:

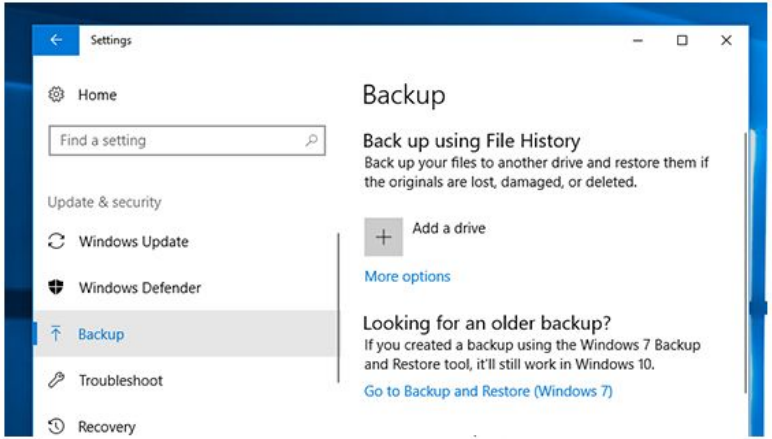
- Em Configurações, clique em “Conversas” e, em seguida, em “Backup de Conversas”
- Ative a criptografia de ponta a ponta
(opção “Backup criptografado de ponta a ponta”)
- Confirme as informações sobre sua senha
(senha de restauração do backup)
- Crie e confirme sua senha
- Toque no botão “Criar” para habilitar o backup criptografado de ponta a ponta no WhatsApp

Backups

Windows 10

- Em Configurações, clique em “Atualização e segurança” e depois em “Backup”

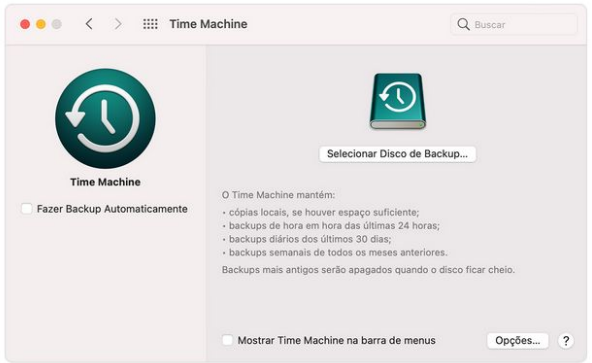
- Clique em “Adicionar uma unidade” e selecione um HD externo ou um computador de rede para configurar o backup periódico



Backups

MacOS

- Abra as preferências Time Machine no menu do Time Machine na barra de menus
OU
Selecione o menu Apple > Preferências do Sistema e clique em “Time Machine”
- Clique em "Selecionar Disco de Backup" e selecione seu disco de backup na lista de discos disponíveis.

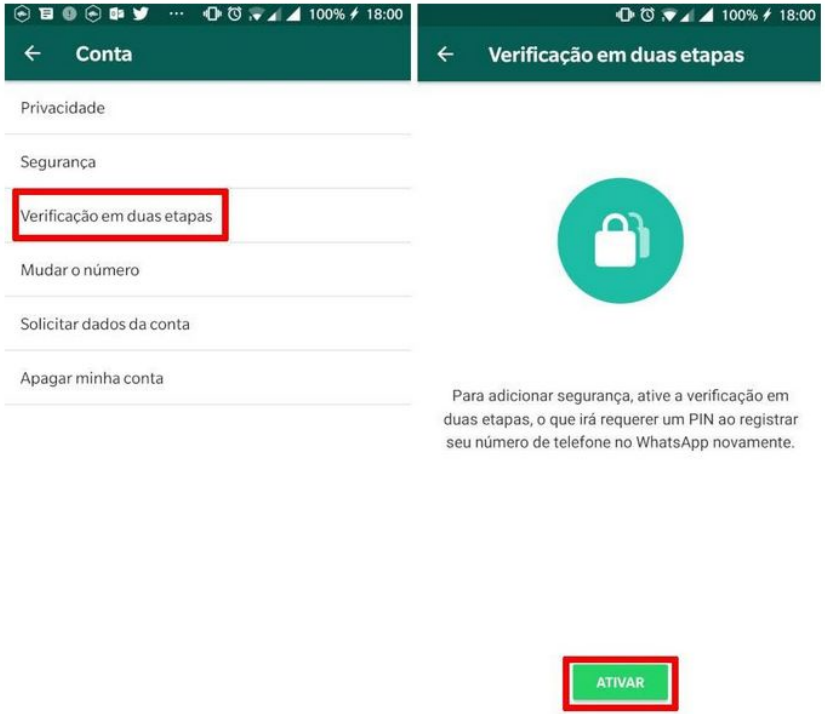


- Para disponibilizar seu backup apenas para os usuários que têm a senha de backup, você pode selecionar "Criptografar backups". Em seguida, clicar em Usar Disco.

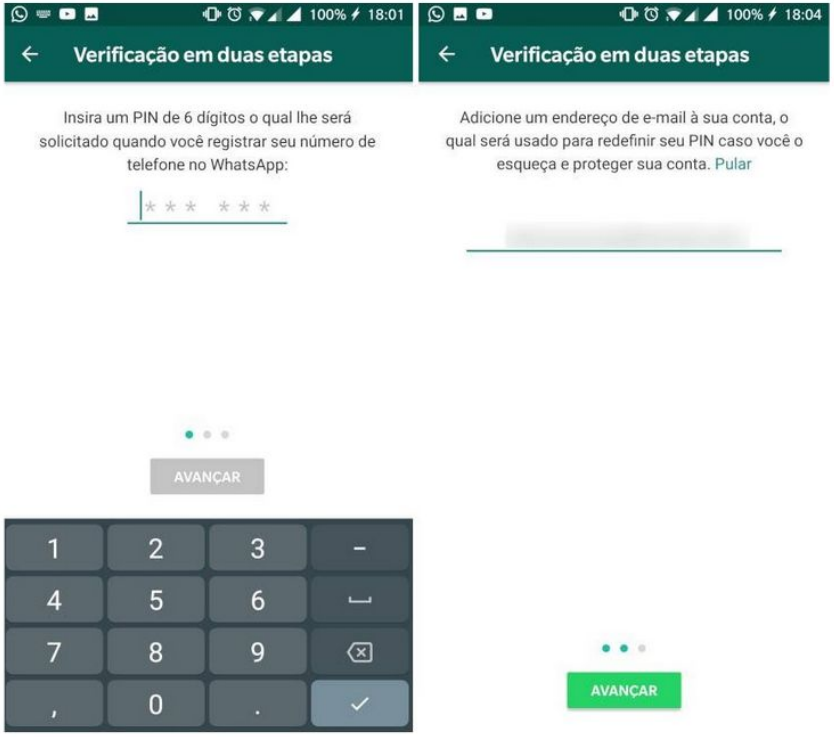
Gerenciador de senhas

- Software livre / Open Source:
  - Bitwarden: https://bitwarden.com/
  - NordPass: https://nordpass.com/
  - KeePassXC: https://keepassxc.org/, multiplataforma
  - Keepas2Android
  - KyPass para iPhone
- Soluções proprietárias, “na nuvem” e com opções para equipes:
  - LastPass
  - 1Password

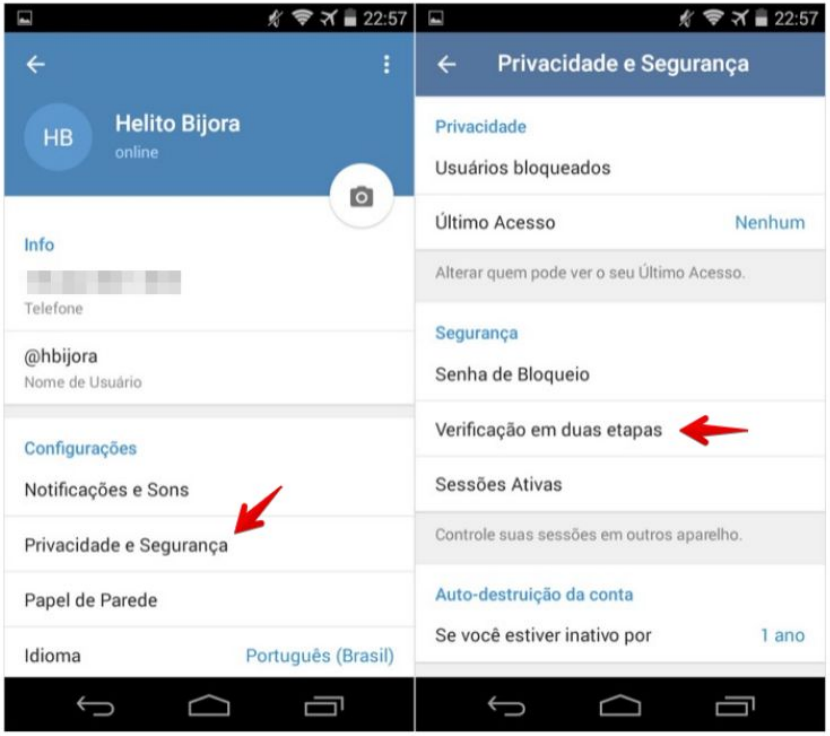
Autenticação em 2 fatores



Autenticação em 2 fatores



Autenticação em 2 fatores



Autenticação em 2 fatores

Saiba mais sobre os métodos 2FA alternativos

10 jan 2019

Nos últimos anos, o conceito de autenticação de dois fatores (2FA), antes uma exclusividade dos nerds, foi se tornando popular. No entanto, o assunto ainda está muito limitado ao uso de 2FA por meio do envio de senhas únicas via SMS. É triste dizer, mas essa não é a opção mais segura. Eis o porquê:

- É fácil espiar as senhas enviadas por SMS se as notificações da tela de bloqueio estiverem habilitadas.
- Mesmo que as notificações estejam desabilitadas, um cartão SIM pode ser removido e instalado em outro smarphone, o que permite o acesso às mensagens SMS com senhas.

Autenticação em 2 fatores

- Mensagens SMS com senhas podem ser interceptadas por um Trojan camuflado dentro do smartphone.
- Usando diversas táticas desleais (persuasão, suborno, etc.), criminosos podem conseguir um novo cartão SIM com o número da vítima em uma loja de celulares. As mensagens SMS então irão para esse cartão.
- Mensagens SMS com senhas podem ser interceptadas por meio de uma falha básica no protocolo SS7 usado na sua transmissão.

Note que até mesmo os métodos mais tecnológicos ou trabalhosos para roubar mensagens SMS com senhas (exploração do SS7) dos mencionados acima já foram colocados em prática. O restante faz parte da rotina diária dos cibercriminosos. Dito isto, não estamos lidando com uma ameaça hipotética, mas real.

Fonte: "Saiba mais sobre os métodos 2FA alternativos" Por Alex Drozhzhin, 10/01/2019, em Kaspersky Daily

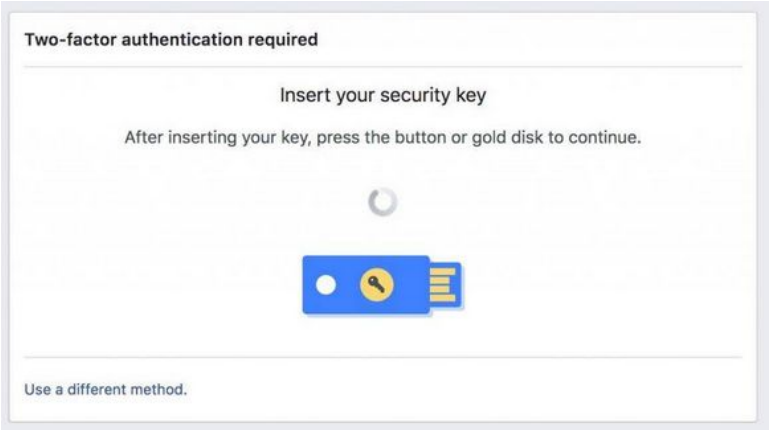
Autenticação em 2 fatores

- Aplicativos de autenticação
  - Authy - Plataformas suportadas: Android, iOS, Windows, macOS, Chrome
  - FreeOTP - Plataformas suportadas: Android, iOS
  - Duo Mobile - Plataformas suportadas: Android, iOS
  - Google Authenticator - Plataformas suportadas: Android, iOS
  - Microsoft Authenticator - Plataformas suportadas: Android, iOS

Fonte: "Saiba mais sobre os métodos 2FA alternativos" Por Alex Drozhzhin, 10/01/2019, em Kaspersky Daily

Autenticação em 2 fatores

- Tokens de hardware com base no padrão U2F (Universal 2nd Factor), criado pela FIDO Alliance



Fonte: "Saiba mais sobre os métodos 2FA alternativos" Por Alex Drozhzhin, 10/01/2019, em Kaspersky Daily

VPN (virtual private network)

Uma VPN oculta seu endereço IP deixando que a rede redirecione você por meio de um servidor remoto

- Principais benefícios:
  - Disfarça seu paradeiro
  - Proporciona transferência segura de dados
- Como uma boa VPN atua?
  - Criptografia do seu endereço IP e de protocolos
  - “Kill switch”
  - Autenticação de dois fatores

VPN (virtual private network)

5 Best No Logs VPN Services that are Verified & Proven

October 19, 2021 *By* Sven Taylor — 39 Comments

	Verified No Logs VPNs:
1	NordVPN
2	ExpressVPN
3	VyprVPN
4	Perfect Privacy
5	OVPN

Fonte: **"5 Best No Logs VPN Services that are Verified & Proven" Por Sven Taylor, 19/10/2021, Em Restore Privacy**

Apps de vídeoconferência mais seguros

O mais indicado : https://bbb42.de/b

BigBlueButton é um sistema de webconferência de código aberto para aprendizagem on-line. BigBlueButton permite que você compartilhe documentos (PDF e qualquer documento de escritório), webcams, bate-papo, áudio e sua área de trabalho. Ele também pode gravar sessões para reprodução posterior.

Workshop - Introdução à Segurança Digital

Perguntas & Respostas & Debate

Coda-Br 2021

Workshop - Introdução à Segurança Digital

Haydée Svab
@hsvab
hsvab@ask-ar.xyz

Nina da Hora
@ninadhora

Coda-Br 2021