100 DICAS

DE SEGURANÇA DA INFORMAÇÃO

Para todos aqueles que usam
a internet no seu dia a dia.

por Emílio Arimatea

DADOS DE ODINRIGHT

Sobre a obra:

A presente obra é disponibilizada pela equipe ***eLivros*** e seus diversos parceiros, com o objetivo de oferecer conteúdo para uso parcial em pesquisas e estudos acadêmicos, bem como o simples teste da qualidade da obra, com o fim exclusivo de compra futura.

É expressamente proibida e totalmente repudíavel a venda, aluguel, ou quaisquer uso comercial do presente conteúdo.

Sobre nós:

O ***eLivros*** e seus parceiros disponibilizam conteúdo de dominio publico e propriedade intelectual de forma totalmente gratuita, por acreditar que o conhecimento e a educação devem ser acessíveis e livres a toda e qualquer pessoa. Você pode encontrar mais obras em nosso site: ***eLivros***.

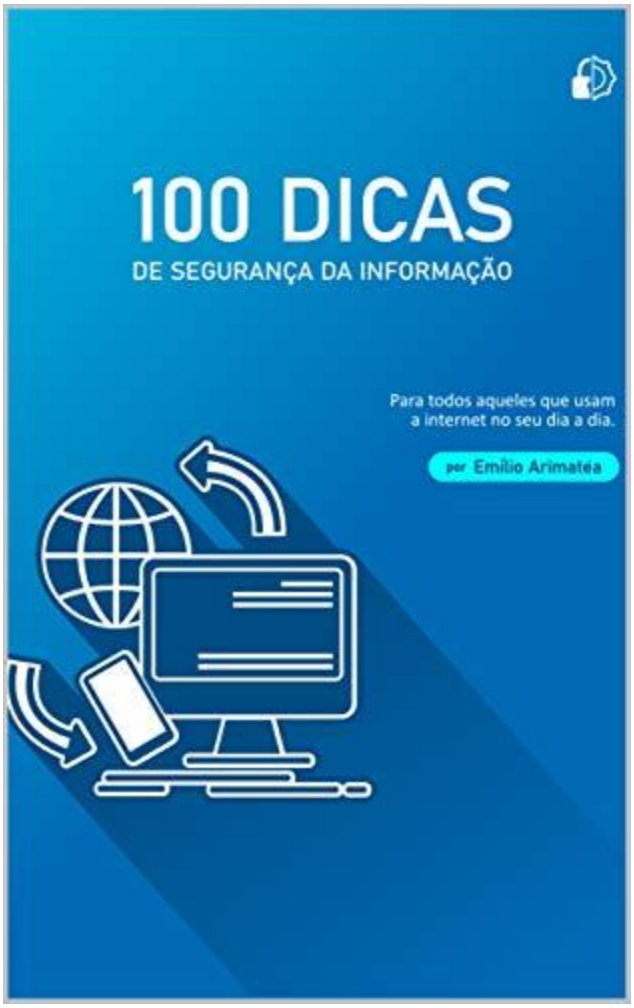
Como posso contribuir?

Você pode ajudar contribuindo de várias maneiras, enviando livros para gente postar ***Envie um livro*** ;)

Ou ainda podendo ajudar financeiramente a pagar custo de servidores e obras que compramos para postar, ***faça uma doação aqui*** :)

"Quando o mundo estiver unido na busca do conhecimento, e não mais lutando por dinheiro e

poder, então nossa sociedade poderá enfim evoluir a um novo nível."



DE SEGURANÇA DA INFORMAÇÃO

Para todos aqueles que usam

a internet no seu dia a dia.

ISENÇÃO DE RESPONSABILIDADE

Todas as informações con das neste ebook são provenientes de minhas experiências pessoais e com pesquisas na internet. Todos os nomes de marcas, produtos e serviços mencionados neste ebook são propriedades de seus respec vos donos e são usados somente como referência.

Além disso, em nenhum momento neste guia há a intenção de difamar, desrespeitar, insultar, humilhar ou menosprezar você leitor ou qualquer outra pessoa, cargo ou ins tuição. Caso qualquer escrito seja interpretado dessa maneira, eu gostaria de deixar claro que não houve intenção nenhuma de minha parte em fazer isso. Caso você acredite que alguma parte deste guia seja de alguma forma desrespeitosa ou indevida e deva ser removida ou alterada, pode entrar em contato diretamente comigo através do e-mail **emilioarimatea@gmail.com**.

DIREITOS AUTORAIS

2

Sobre o Autor

Sou Emílio Arimatéa e trabalho há 18 anos com Tecnologia da Informação dos quais 5 foram dedicados a Segurança da Informação. Formado pela universidade Estácio de Sá em redes de computadores e pós-graduado pela Universidade Veiga de Almeida em gestão de projetos com foco em segurança da informação. Fui tutor presencial na disciplina de introdução à

informá ca no CEDERJ e Chefe de segurança da informação no CEFET/RJ.

Possuo Cer ficação (CASE) Cer fied Automa on Security Engineer, (PCCSA) Palo Alto Networks Cer fied Cybersecurity Associate e vários cursos relacionados à área de segurança da informação, tais como: Tratamento de incidentes de segurança, norma ISO 27001 e 27002, etc.

Atualmente, trabalho como Analista em Cibersegurança para Infraestrutura Crí ca.

3

Sumário

Introdução

O acesso à internet tornou-se ro na no dia a dia da maioria da população.

Pagar contas pelo smartphone, publicar em redes sociais, enviar e receber e-mails, pesquisar assuntos variados entre outras facilidades que a internet viabiliza, trouxe um grande ganho de produ vidade e agilidade nas tarefas diárias. Fazemos muito mais coisas e em menos tempo do que em qualquer outra época da nossa história.

Contudo, essa facilidade fez migrar alguns crimes do mundo real para o mundo virtual mudando apenas a forma e o meio de como executá-los.

Roubo de dados pessoais, chantagens pelas redes sociais, fraudes, esses são apenas alguns dos vários crimes come dos pela internet.

O obje vo deste ebook é dar dicas sobre segurança da informação para o público em geral.

Uma parte dos usuários da internet não sabe dos perigos do mau uso dela, uma outra parte sabe dos perigos, mas não se previne ou não se previne o suficiente e somente uma pequena parte faz uso seguro e cauteloso.

Reunimos dicas simples e de fácil entendimento sobre segurança da informação com um intuito de melhorar a prevenção contra criminosos digitais e a segurança no uso da internet, evitando prejuízos e dores de cabeça que, em algumas situações, podem resultar em grandes perdas financeiras, abalo emocional e processos criminais.

Anti-Malware

Mantenha seu programa an -malware atualizado e no modo de atualização automá ca pela rede, incluindo o arquivo de assinatura. Dê preferência para a atualização diária, visto que quanto mais atual a assinatura, mais preparado

#1 para bloquear arquivos maliciosos o an -malware estará.

Sempre que for necessário usar computadores de terceiros, por precaução, u lize um an -malware online antes de usá-lo. Várias empresas de segurança da informação disponibilizam esse serviço gratuitamente, como por exemplo, a Bitdefender, Kaspersky e a F-security. Caso encontre algum malware, a própria

#2 ferramenta já faz a remoção e geralmente emite um relatório do que foi encontrado no computador.

Não é aconselhado executar simultaneamente diferentes programas an -

malware, pois eles podem entrar em conflito e afetar na eficácia de detecção.

Além disso, pode também impactar no desempenho do computador deixando-o

#3 lento.

An gamente os códigos maliciosos u lizavam apenas alguns pos de arquivos (extensões) para se disseminarem, mas hoje eles podem usar qualquer um.

#4 Portanto, configure seus an -malware para examinar todos os formatos, incluindo extensões ocultas.

Configure o seu an -malware para verificar todos os arquivos recebidos, independentemente de onde eles estejam vindo. Muitas infecções acontecem por pessoas conhecidas que na maioria das vezes nem sabem que estão

#5 contaminadas e acabam passando o código malicioso[5] adiante.

A execução de macros (sub-ro nas capazes de executar tarefas pré-

programadas), geralmente em arquivos de programas como os da Microso

(Word, Excel e PowerPoint), pode ser perigoso caso você não tenha certeza de que ele não contém vírus. Somente permita a sua execução quando realmente for necessário.

#6 Uma opção seria u lizar visualizadores gratuitos disponibilizados pelos fabricantes nos próprios sites.

Backup

Não tente recuperar um backup (cópia dos seus arquivos) caso perceba que ele contenha dados não confiáveis devido a um ataque de malware ou a uma alteração indevida. Recupere o backup mais an go do que o que teria sido

#7 comprome do. Se possível, recupere os backups de tempos em tempos para verificar se ele está sendo feito corretamente.

Cartão de Crédito

Use os seus dados bancários com cautela. Somente conceda os números de cartão de crédito quando for realizar transações que requeiram esses dados.

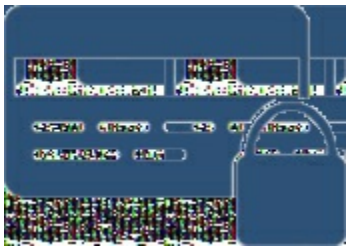
Os mesmos cuidados que você tem com seus dados no mundo real, você

#8 também tem que ter no mundo virtual. Proteja-se.

Se porventura, o seu disposi vo móvel for perdido ou furtado, bloqueie imediatamente os números de cartões de créditos dos quais estejam nele gravados. Tenha, ao seu alcance, o número do telefone da operadora do

#9 seu cartão de créditos para facilitar na hora bloqueá-lo.

7



Cartão de Segurança

Mantenha o seu cartão de segurança[2] em um local seguro e longe de pessoas estranhas. O cartão é único e exclusivo e somente você deverá usá-lo. Ele é u lizado como um item adicional de segurança para acesso às transações

#10 realizadas pelo Internet Banking.

Atenção com o cartão de segurança de acesso a sua conta bancária.

Averigue se o número de iden ficação do cartão mostrado pelo serviço bate com o que está no seu cartão, caso não, entre em contato com o

#11 serviço imediatamente.

No uso do cartão de segurança, informe somente uma posição por cada acesso ou transação realizado. Caso seja digitada uma chave incorreta, será solicitada posteriormente a chave da mesma posição e não outra,

#12 até que se digite a numeração corretamente. Usando o cartão corretamente, diminui bastante fraudes no acesso as contas bancárias.

8

Computadores

Assuma uma postura preven va ao usar o seu computador. Tenha cuidado ao manusear os seus arquivos e quando navegar pela internet. Apesar das atualizações de segurança estarem disponíveis cada vez mais rápido, novos

#13 malware surgem a cada minuto e nem sempre as ferramentas de segurança conseguem acompanhar.

Nunca use opções como “Con nuar conectado” e “Lembre-se de mim”

em computadores de terceiros (lan house, computador de um amigo, computador da biblioteca etc). Quando você usa essas opções, você deixa as informações da sua conta de usuário e senha salvas em cookies

#14 que podem ser indevidamente coletados e permitem que outras pessoas se auten quem como se fosse você.

A maioria dos programas de computadores (navegadores, leitores de PDF, leitores de e-mails etc) disponibilizam configurações de segurança e privacidade, porém, a maioria vem desabilitada por padrão ou em níveis considerados baixos pelos ataques atuais. Habilite as configurações

#15 de acordo com as suas necessidades mantendo os programas sempre atualizados com as correções de segurança.

Quando precisar enviar seu computador para a manutenção, confirme se os programas que serão instalados são originais. Caso não tenha condições de adquirir a licença, opte por programas gratuitos seme-lhantes aos que deseja usar. Existem diversos programas gratuitos,

#16 de qualidade, que tem pra camente as mesmas funções que os programas pagos.

Fique atento à data e a hora do seu computador, mantenha-os sempre atualizado.

A data e a hora estão relacionadas diretamente com itens de segurança da informação (cer ficado digital[3], incidentes de segurança, logs [13], atualização dos programas, entre outros). Windows, Linux e Mac possuem suporte para a

#17 sincronização de horário através da internet.

Tenha cuidado ao u lizar computadores de terceiros, pois eles podem estar infectados sem que você o saiba. Caso desconfie de algo, não o u lize e comunique ao dono do equipamento. Isso evita, por exemplo, que suas

#18 senhas sejam ob das indevidamente e seus aplica vos sejam acessados.

Ao u lizar computadores em público, procure cuidar da sua segurança sica, visto que ele poderá ser roubado em todo ou em partes. Use travas para impedir que ele seja aberto e cabos de aço para que ele não seja levado

#19 indevidamente.

Computador mais lento para acessar a rede e gravando ou lendo com muita frequência o disco rígido, é um indício de que ele possa estar com problemas de segurança. Confira se ele está seguro verificando os logs, escaneando com

#20 um an -malware, entre outras ações.

A conta de administrador do Windows lhe permite fazer qualquer po de alteração no computador, portanto, somente u lize quando for estritamente necessário. Usando essa conta, você estará exposto à instalação de malware

#21 que justamente precisam destas permissões para, além de se instalar, se replicar e fazer diversas outras alterações no Windows.

Situações em que você necessite de privilégios administra vos no seu computador, u lize a opção de executar como administrador e no mínimo tempo possível. Dessa forma, você evita que um malware seja instalado em

#22 seu computador e execute ações privilegiadas.

10

Tenha sempre um disco de emergência para u lizar em situações como: computador agindo de modo anormal, muito lento e com muito acesso ao

disco rígido. Lembrando

#23 sempre de fazer backup dos seus arquivos pessoais com frequência.

Observe sempre os logs[13] do seu computador pois dependendo do que es ver registrado nele, será possível apontar tenta vas de acesso indevido, ataques e roubo de dados. Eles também são importantes para o rastreio de ações

#24 executadas por um invasor para ocultar os seus registros (cópia e deleção de arquivos, comandos, entre outros).

Garanta que os programas que você u liza e o sistema operacional sempre estejam com as versões mais recentes, deste modo, você evita que vulnerabilidades sejam exploradas pelos atacantes. Configure, quando disponível, para que os programas sejam atualizados automa camente.

#25 Em casos de programas que não possuem esse recurso, consulte sempre os sites dos fabricantes para verificar se há novas atualizações.

Efetue logout (sair) de sua conta de usuário, em todos os sites que você tenha acessado, sempre que u lizar computadores de terceiros. Em computadores de terceiros não se sabe se são aplicadas as medidas de proteção que

#26 normalmente aplicamos em nossos computadores pessoais, portanto, ele pode estar vulnerável a vírus e a ataque de hackers.

Cookies

Cookie é um pequeno arquivo de computador ou pacote de dados enviados por um site de internet para o navegador do usuário, quando ele visita o site. Tenha cuidado ao usar os cookies, uma vez que eles podem ser usados para seguir e manter as suas preferências de navegação. Ajuste o seu navegador para que ele

#27 apague os cookies assim que for fechado.

Gere uma lista de exceções de definições de cookies para sites considerados confiáveis (Internet Banking, e-commerce, webmail, entre outros.). Os demais sites deixe bloqueado para definição de cookies. Isso

evita que sites não

#28 confiáveis definam cookies em seus navegadores evitando rastreio de suas a vidades na internet.

11

Criptografia

Faça o uso de criptografia[7] nas aplicações quando for u lizar rede sem fio,

#29 por exemplo: VPN[17] para conexões remotas e HTTPS[11] para acesso via webmail. A auten cação e a criptografia entre o cliente (você) e o AP

(Access Point) também se faz necessário.

Em situações as quais se deseja assegurar ao des natário que o conteúdo de uma mensagem não seja alterado, u lize assinatura digital. Ela permite comprovar a auten cidade (foi realmente criada por quem diz ter feito)

#30 e a integridade (não foi alterada) de uma mensagem.

12

Ao usar um leitor de e-mails, u lize criptografia entre ele o leitor e os

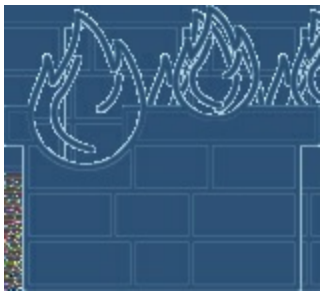
#31 servidores do seu provedor. Geralmente os provedores disponibilizam, no próprio site, um passo a passo para configurar a criptografia e assim aumentar a segurança.

Quando os acessos aos sites con verem fornecimento de senhas, u lize

#32 serviços criptografados, dado que protege as conexões contra acessos indevidos. Evite sites que não forneçam esse po de serviço, em casos, como já citado, que envolvem uso de senhas.

Crie um arquivo em seu computador e insira suas contas (logins/senhas).

#33 Logo após, criptografe com algum programa disponível na internet (encrypto, veracrypt, entre outros). A senha de criptografia tem que ser bem forte, pois se algo acontecer com ela, as senhas armazenadas estarão comprome das.



Firewall

Instale um firewall[8] pessoal em seu computador, em conjunto ou não, com um an -malware. Observe, regularmente, os logs[11] gerados pelo firewall, an -malware e o sistema operacional do seu computador. Essa verificação ajuda a descobrir se há algum registro que possa indicar, por exemplo,

#47 tenta vas de invasão.

Para acessos domés cos via banda larga, instale um firewall entre a rede interna e a internet. Dessa forma, você protege seus equipamentos de acessos externos, pois o firewall não deixará passar tráfego com origem

#48 na internet e des no a rede interna, onde estão localizados seus disposi vos.

Dispositivo Móvel

Caso perca seu disposi vo bluetooth[1] remova as relações de confiança que os outros disposi vos já haviam estabelecido com ele. Isso evita que quem

#34 achar o seu disposi vo perdido u lize-o para conectar com os seus outros disposi vos e roubar dados como fotos, vídeos e textos. Dependendo do disposi vo que ele se conectar, poderia também inserir um vírus para monitorá-lo pela internet.

Altere, sempre que possível, a senha (PIN) padrão do seu disposi vo bluetooth[1]. Normalmente essa senha fica disponível nos sites dos fabricantes e na própria embalagem do disposi vo. Para evitar que alguém

#35 tente u lizá-la indevidamente para acessar seu disposi vo, troque-a por uma mais forte.

Auferir disposi vo móvel desbloqueado ilegalmente culminará na perda da garan a do equipamento, visto que essa prá ca é um ato ilícito. Além disso, a segurança também estará comprome da, já que o acesso às configurações restritas do aparelho foi violado. Pense duas vezes antes de obter um dispo-

#36 si vo móvel nessas condições.

Verifique sempre as no cias sobre segurança no site do fabricante do seu disposi vo móvel. Normalmente eles disponibilizam uma seção específica no site para comentar sobre atualizações, vulnerabilidades, entre outros

#37 assuntos relacionados à segurança da informação. Mantenha seu aparelho sempre atualizado.

Não compre disposi vo móvel com permissões de acesso modificadas, visto que isso viola os termos de garan a, afetará a segurança e também o funcionamento correto do equipamento. O barato pode sair caro, pois você

#38 corre o risco, entre outros, de ter seus dados pessoais expostos.

Em situações de perda/furto de seu disposi vo móvel, entre em contato o mais rápido possível com a sua operadora e solicite o bloqueio da linha.

Somente é necessário o fornecimento do número da linha para operadora,

mas é interessante você também ter o número do IMEI (Interna onal

#39 Mobile Equipment Iden ty), um número de iden ficação único de cada disposi vo móvel.

Fique atento ao instalar aplicações desenvolvidas por terceiros, visto que

#40 não há nenhuma garan a que ela foi feita de maneira segura ou se foi desenvolvida para fins maliciosos, como roubar dados para acesso ao internet banking. Instale aplicações de fontes confiáveis e verifique sempre as avaliações dos usuários.

Email

Seja cauteloso ao ceder seu endereço de e-mail. Algumas ações podem ser tomadas para diminuir a quan dade de spams recebidos. Uma delas é criar contas de e-mail secundárias para fornecer em locais onde as chances de

#41 receber spam são grandes, por exemplo, ao preencher cadastro em listas de discussão, bole ns informa vos, entre outros.

Ao enviar mensagens para muitos des natários, u lize a alterna va ”Bcc”

ou “Cco” (com cópia oculta), pois evita que outras pessoas vejam os endereços de e-mails da mensagem. Destarte, você preserva o e-mail das

#42 pessoas e resguarda a privacidade delas.

Muito cuidado quando forem usar leitores de e-mails. Desa ve as opções que liberam abrir automa camente arquivos ou programas anexados às mensagens, assim como a opção de execução de Java Script[12]. Isso evita que códigos maliciosos se auto executem assim que forem abertos pelo seu

#43 leitor de e-mails e por conseguinte infectem o seu computador ou disposi vo móvel.

A ve, quando possível, o seu leitor de e-mails para marcar as mensagens suspeitas de serem fraude. Normalmente e-mails que envolvam contas

#44 bancárias internacionais, que precise enviar seus dados bancários para o exterior ou dizendo que você

ganhou um sorteio, entre outros, há indícios que é uma fraude.

Para evitar que um spammer iden fique que o e-mail que ele enviou foi lido por você, desa ve a abertura de imagens em e-mails HTML[9]. Não sabendo que o e-mail foi lido, ele não terá certeza que o seu e-mail é válido.

#45 Isso serve tanto para acesso via navegador quanto para leitores de e-mails.

Boa parte dos sistemas não usa criptografia em seus sistemas. Quando os **15**

usuários desse sistema solicitam o reenvio da senha de acesso, elas são enviadas em texto claro. A dica é, assim que receber essas senhas por e-

mail,

#46 altere-as o quanto antes, pois corre o risco de elas serem interceptadas e u lizadas indevidamente.

Internet

Sempre que u lizar rede sem fio em locais públicos, use serviços que

#49 u lizem conexão segura (HTTPS). Evite usar a rede sem fio dos locais que não possuem esse po de conexão, mesmo que você já conheça o estabelecimento

Quando for trafegar dados sigilosos (senhas, números de cartão de crédito, informações bancárias etc.) na internet, u lize “HTTPS”[11] ao invés do

“HTTP”[10], já que este não garante que sua comunicação esteja segura ou até mesmo que ela seja no site requisitado. Caso o site não forneça

#50 conexões seguras “HTTPS”[11] mesmo manipulando dados sigilosos como citado anteriormente, por precaução, não o u lize.

Fique atento com os golpes que acontecem na internet. Todos eles são similares àqueles que são aplicados em locais sicos ou por telefone.

Sendo assim, os riscos também são os mesmos presentes no nosso co diano.

#51 Os golpes sempre vão ocorrer, só mudam o local e os atores e a maneira de fazer.

Tenha cuidado ao usar a internet. Ela deve ser u lizada com cautela e atenção. Insira a segurança da informação em sua ro na, independente de questões como local de onde está acessando, tecnologia u lizada e

#52 equipamento. Dessa forma, você irá reduzir o risco de ter algum problema relacionado à segurança da informação e roubo de dados.

Antes de fazer compras na internet, verifique se a empresa não tem

reclamações em sites especializados em reclamações de consumidores.

#53 Além disso, verifique se o site possui o “cadeado do navegador”

exibido na barra de status do programa. Ele indica que todas as informações fornecidas são criptografadas e ninguém, além do próprio sistema, poderá acessá-las.

Proteja-se de fraudes na internet. Suspeite de mensagens contendo enormes bene cios, por exemplo, quando pedem para fazer algum

#54 pagamento com a promessa de receber um valor maior. Esse po de mensagem nunca deve ser respondida, visto que isso pode confirmar que o seu endereço de e-mail é válido e poderá ser usado futuramente para outros pos de golpe.

Sempre que for realizar compras na internet, não forneça dados de pagamentos caso o site não disponibilize conexão segura (HTTPS[11])

para transferência dos dados. Se você fornecer seus dados de pagamentos em uma conexão não segura, corre o risco dos seus dados

#55 serem interceptados e u lizados posteriormente para fazerem compras em seu nome.

Nunca u lize sites de busca e links dentro de páginas ou mensagens para acessar sites de comércio eletrônico. Caso conheça a URL[15] digite-a no próprio navegador Web. Dessa maneira, você evita ser direcionado para

#56 um site falso e, caso faça compras por ele, ter seus dados bancários roubados.

Existe muito conteúdo fake na internet, fique atento para não compar lhar informações falsas. Pesquise em fontes de informações confiáveis e em mais de uma, verifique a data da no cia e desconfie de matérias

#57 sensacionalistas. Compar lhar fake news é crime, tanto para quem as cria quanto para quem as compar lha.

Para sites importantes que requerem uma maior privacidade e cuido

#58 com os dados pessoais, u lize navegação anônima disponibilizadas pelos navegadores web (google chrome, firefox, edge etc). Dessa forma, informações de sites, cookies e formulários não são gravadas pelo navegador evitando serem rastreados por terceiros Antes de instalar um módulo de segurança de qualquer Internet Banking,

#59 cer fique-se de que o autor do módulo é realmente a ins tuição em questão. Geralmente as ins tuições disponibilizam informações sobre segurança da informação no próprio site ou por telefone via SAC.

Tenha cuidado ao acessar sites de Internet Banking ou de comércio eletrônico. Mantenha a Webcam (caso você possua uma) desligada sempre que for acessar esses sites. Se você ver um notebook,

#60 instale um protetor de Webcam nele e só abra quando for u lizá-la.

Quando for usar sites de leilão e/ou de venda de produtos faça uso de sistemas de gerenciamento de pagamentos, já que dessa forma você dificulta a aplicação de golpes e também impede que seus dados sejam

#61 encaminhados aos golpistas. Além disso, você pode confirmar o pagamento diretamente no próprio sistema que é mais seguro.

Privacidade

No meio de inúmeras no cias que circulam nas mídias sociais fica duvidoso saber no que acreditar. Fique alerta para não ser enganado por boatos e

#62 acabar compar lhando informações falsas. Conhecidas como hoaxes, correntes e fake news, costumam se espalhar rapidamente pelas redes sociais e podem causar muitos danos a sociedade. Na dúvida, consulte os sites para verificar a veracidade da informação: Boatos.org -

h p://www.boatos.org / E-farsas - h p://www.e-farsas.com, entre outros.

Mantenha seu ambiente profissional resguardado. Analise, antes de revelar uma informação publicamente, se ela afetará nega vamente a imagem da empresa e por consequência a sua também. Além de não ser bom para a

#63 imagem da empresa, essa informação pode ser usada por algum atacante que esteja coletando informações para um futuro ataque direcionado.

Aconselhe seus filhos a nunca marcarem encontros com pessoas estranhas na internet. Devido a elas serem expostas e de fácil manipulação, tornam-se alvo nas redes sociais. Mantenha seus filhos sempre informados dos perigos

#64 e fique de olho por onde eles navegam e com quem eles falam na internet.

Preze pela privacidade dos outros. Tenha cuidado ao comentar sobre as ro nas e hábitos delas. Evite divulgar imagens ou mensagens copiadas de

#65 perfis sem a autorização das mesmas, mesmo que os perfis sejam públicos.

Para sites importantes que requerem uma maior privacidade e cuido com

#66 os dados pessoais, u lize navegação anônima disponibilizadas pelos navegadores web (google chrome, firefox, edge, etc). Dessa forma, informações de sites, cookies e formulários não são gravadas pelo navegador evitando serem rastreados por terceiros **18**

Programas

Cer fique-se de manter sempre o seu programa de distribuição de arquivos

#67 atualizado. Normalmente os próprios programas alertam que existem atualizações a serem baixadas e instaladas. Configurá-lo corretamente também é uma boa prá ca para mantê-lo seguro.

Antes de usar programas de distribuição de arquivos (P2P[14]), verifique se os arquivos ob dos/distribuídos não violam as leis de direitos autorais.

Com uma simples pesquisa na internet você pode verificar se o arquivo

#68 possui ou não direitos autorais. Caso possua, entre em contato com os autores solicitando permissão para compar lhar.

Mantenha seus programas sempre atualizados com as correções de segurança disponibilizadas pelos fabricantes, incluindo o sistemas operacional, firewall e an -malware. Em programas que não tem a opção

#69 de no ficar o usuário sobre a atualização, crie uma ro na para você mesmo verificar diretamente no site do fabricante. (Ex. uma vez por semana).

Verifique sempre se o seu computador está com vulnerabilidades em algum programa. Existem programas que fazem essa inspeção para você e apontam quais precisam ser atualizados. Se preferir, você pode fazer

#70 manualmente. De qualquer forma, não deixe de verificar se os programas estão atualizados.

19

Ransomware

Ransomware é um so ware malicioso que criptografa os dados

#71 armazenados em seu computador e exige um pagamento de resgate para liberá-los. Normalmente o resgate é exigido em bitcoin. Tenha sempre backups dos seus arquivos fora do computador, para que em casos de uma infecção por ransomware, você ter a possibilidade de recuperá-los.

Para se proteger de um ransomware, basta você ter os mesmos cuidados que já tem contra outros pos de códigos maliciosos, por exemplo: instalar e manter atualizado um an vírus, manter atualizado o sistema operacional

#72 e os programas, entre outros. Faça backup sempre, pois também é uma forma de proteção contra o ransomware.

Redes sem fio

Na instalação de rede Wi-fi residencial troque as senhas originais de fábrica, visto que elas fáceis de descobrir. Mude tanto a senha de acesso administra vo com a auten cação do usuário. Coloque senhas fortes em

#73 ambos os acessos e não se esqueça de trocá-las regularmente, principalmente a de auten cação do usuário.

20

Redes Sociais

Habilite as no ficações de login nas redes sociais. Dessa forma, fica mais fácil perceber acessos indevidos ao seu perfil. Caso iden fique uma invasão, denuncie o quanto antes. Nas próprias redes sociais você encontra opções

#74 para fazer a denúncia.

Nunca repasse mensagens sem antes verificar se ela é verdadeira ou falsa.

Nem tudo que você lê nas redes sociais é verdade, principalmente quando as mensagens têm o obje vo de chamar muito a atenção. Por exemplo:

“repasse para todos seus contatos”, “Algo ruim irá lhe acontecer se você

#75 não compar lhar” ou “Você ganhará um prêmio se repassar a mensagem”.

Existem muitas outras similares, fique atento.

Cuidado ao usar redes sociais baseadas em geolocalização. Faça o check-in[4] em locais movimentados e conhecidos e nunca em locais perigosos ou com pouco movimento. Além disso, faça o check-in[4]

quando es ver saindo do local e não quando es ver chegando. Isso

#76 dificulta com que pessoas mal-intencionadas que estão a sua procura, localizem-no.

Tente limitar quem pode ter acesso ao seu endereço de e-mail, uma vez que grande parte dos spammers usam esses

dados para abastecer listas de envio de spam. Algumas redes permitem esconder o endereço de e-mail ou delimitar as pessoas que terão acesso a ele. Cuide da sua

#77 privacidade.

Preserve sua vida profissional, pois ela pode atrapalhar em um processo sele vo que você venha a par cipar. U lize redes sociais para fins específicos, por exemplo: uma para assuntos profissionais (linkedin) e outra para o lazer (instagram). Dessa forma, você evita problemas tanto

#78 em processos sele vos quanto já exercendo alguma função em alguma empresa.

Cuidado ao mostrar sua vida na internet, principalmente nas redes sociais.

A maioria delas (Facebook, twi er, instagram, etc.) fornece configurações

#79 de segurança e privacidade bem fáceis de serem aplicadas.

Senhas

Elabore suas senhas u lizando frases longas, mas que seja de fácil lembrança e que faça algum sen do para você. U lize diferentes pos de caracteres e evite citações comuns, por exemplo, frases populares.

Subs tuições de caracteres reforçam as senhas, por exemplo, subs tua

#80 o “S” pelo “$” e o “a” pelo “@” e assim por diante. Monte o seu próprio padrão de subs tuição de carácter.

Troque suas senhas periodicamente, mas atenção para a frequência.

Períodos muito curtos, por exemplo, uma vez por mês, não é indicado, pois a possibilidade de você colocar uma senha fraca é grande, justamente para não esquecer. Por outro lado, trocar em um período de um ano ou

#81 mais, também não é indicado, visto que se nesse período alguém descobrir ele terá bastante tempo para u lizá-la indevidamente.

O tempo médio na maioria das situações é de seis meses para a troca.

Não reu lize a mesma senha para todos os serviços que você acessa.

Caso um atacante descubra-a, todos os serviços estarão comprome dos e ele poderá acessá-los. Para facilitar, crie grupos de senhas para cada

#82 finalidade, por exemplo: uma para acesso aos serviços de e-mails e outra para acesso às redes sociais.

Na elaboração de senhas, evite senhas relacionadas à proximidade

#83 entre os caracteres, tais como: 1qaz2wsx e QwerTAsdfG. Além de serem já bem conhecidas, podem ser facilmente observadas ao serem

digitadas.

Você deve manter uma regularidade na alteração de suas senhas, mas

#84 sempre que perceber que ela pode ter sido descoberta, não espere por esse período, troque-a o mais rápido possível. Caso use essa mesma senha para outros locais, altere-a em todos eles também.

Tenha atenção ao criar suas senhas. Não u lize na elaboração delas

#85 dados pessoais, tais como: nomes e sobrenomes, números de documentos e cartões de crédito, data de nascimento, placas de carro, nome de animais de es mação, entre outros. Alguns desses dados são facilmente ob dos nas suas redes sociais, portanto, previna-se.

Não use perguntas de segurança que possam ser facilmente descobertas, tais como: o nome do seu me de futebol, nome da sua mãe, nome do seu

filho, entre outros. Crie suas próprias perguntas, mas com respostas

#86 falsas. Ex. caso você goste de viajar e seu país favorito seja a Itália, pode criar a pergunta: “Qual o seu país favorito?” e colocar a resposta

“França”.

O uso da mesma senha para todos os serviços que você acessa enfraquece a segurança, visto que em situações de vazamento de apenas uma senha de algum serviço que você u liza, o atacante irá inferir que você também

#87 usa a mesma senha para outros serviços.

Caso u lize uma mesma senha em mais de uma lugar e suspeitar que ela tenha sido descoberta, troque o mais rápido possível em todos os locais em que ela é usada. O mais indicado é não usar a mesma senha para todos

#88 os locais, posto que os atacantes sempre a testam em outros serviços do mesmo usuário.

Dica de criação de senha: fundamente-se em uma frase e selecione a primeira ou a úl ma letra de cada palavra. Ex. “segurançA da informaçãO

#89 é muito importante parA todoS aqueleS que usam a interneT” a senha poderia ser “AOoeASSemT@”. Números e símbolos também são indicados para acrescentar maior dificuldade em serem descobertas por atacantes.

Não acredite apenas na classificação de complexidade das senhas mostrada

#90 nos sites em geral. Somente você pode definir se a sua senha é realmente boa. Use esse site para testar se a sua senha está forte: h ps://testedesenha.com.br/.

Para melhor administrar suas senhas, u lize um programa gerenciador

#91 de senhas (Keepass, Lastpass, entre outros). Lembrando-se de baixá-lo de uma fonte confiável. Mantenha-o sempre atualizado assim como os demais programas e aplica vos que você u liza.

Dica de criação de senha: tenha um padrão próprio de subs tuição de

#92 caracteres, quanto mais “desorganizada” for a senha melhor, pois dificulta a sua descoberta. Tente misturar números, sinais de pontuação, letras maiúsculas e letras minúsculas.

Dica de criação de senha: quanto mais aleatório forem os caracteres

#93 numéricos, em programas que usam somente esse po de caractere, melhor. Evite sequências do po: 123456789, 987654321, 11111111, 123321, entre outros.

Atenção na geração da chave mestra ao u lizar programas gerenciadores

#94 de senhas, uma vez que a segurança de todas as outras senhas inseridas no gerenciador depende dela. Como ela é a principal, requer uma atenção redobrada.

Quando comprar e for instalar equipamentos de redes (access point, roteador, disposi vos bluetooth, entre outros), troque a senha, pois eles vêm configurados com senha padrão que é facilmente encontrada na

#95 internet (site dos fabricantes, fóruns, etc).

Na elaboração de senhas, não use como parâmetro listas públicas, tais como: nomes de músicas em geral, filmes, séries, idiomas etc. Essas listas são usadas pelos atacantes combinando umas com as outras para tentar

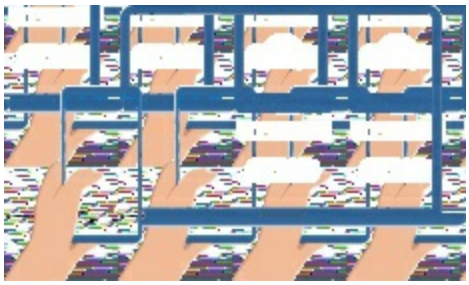
#96 descobrir as senhas das ví mas, para isso, eles suam programas que fazem a combinação automa camente.

Ao anotar suas senhas em um papel, o que não é muito indicado, não o deixe em lugares muito visíveis, como por exemplo: colado no monitor, embaixo do teclado e sobre a mesa. O correto seria memorizar, mas se

#97 mesmo assim você decidir por anotar, coloque em um local trancado que só você tenha acesso.

28

24



Verificação em duas etapas

Fique atento quando u lizar verificação em duas etapas [16] nos seus equipamentos. Caso você perca ou troque o seu celular, não se esqueça de removê-lo da lista de disposi vos confiáveis e cancele os códigos

#98 gerados para os acessos realizados por meio dele. Dessa maneira, você evita o acesso aos outros disposi vos confiáveis.

Verificação em duas etapas ou auten cação em dois fatores (2FA); dificulta a ação de criminosos na tenta va de acessar os seus dados.

A ve-o em todos os serviços os quais ele está disponível ou pelo

#99 menos nos serviços mais importantes/crí cos (e-mail, internet banking etc).

Sempre que u lizar auten cação em dois fatores, lembre-se de manter as informações (e-mail, número do telefone celular, entre outros.) para o recebimento do código de segurança, atualizadas. Caso o código seja

#100 enviado por SMS para um número que não seja mais o seu, você não terá acesso e consequentemente não conseguirá se auten car.

25

Conclusões finais

Os crimes ciberné cos[6] estão aumentando exponencialmente, mas somente uma pequena parte são divulgados nos grandes meios de comunicação. Pesquise mais sobre o assunto em sites de tecnologia da informação e segurança da informação. As 100 dicas de segurança da informação descritas neste ebook cobrem somente uma parte dos assuntos, visto que os ataques, as vulnerabilidades e as formas de proteção são

dinâmicas e algumas mudam com o passar do tempo. Contudo, as dicas con das nesta obra já ajudam bastante a elevar o nível de proteção dos dados pessoas e ao uso seguro da internet.

Espero ter ajudado e caso tenham alguma dúvida, crí ca ou sugestão, fiquem à vontade para entrar em contato comigo por e-mail: emilioarimatea@gmail.com.

Redes sociais:

twi er.com/emilioarimatea

linkedin.com/in/emilio-arimatea

instagram.com/emilioarimatea

26

Referências

Boatos. Disponível em: <h ps://www.boatos.org/>.

Acesso em: 29 de set. 2019.

Car lhas Cert.br. Disponível em: <h ps://car lha.cert.br/>.

Acesso em: 28 de agosto. 2019.

E-farsas. Disponível em: <h p://www.e-farsas.com/>.

Acesso em 16 de set. 2019.

Empresa Brasil de Comunicação. Disponível em: <h p://www.ebc.com.br/tecnologia/>.

Acesso em 24 de ago. 2019.

Ins tuto Nacional de Tecnologia da Informação. Disponível em: <h ps://www.i .gov.br/glossario>.

Acesso em 30 de ago. 2019.

Significados. Disponível em: <h ps://www.significados.com.br/>.

Acesso em 31 de ago. 2019.

Teste de senha. Disponível em: <h ps://testedesenha.com.br/>.

Acesso em 10 de set. 2019.

Glossário

[1] Bluetooth: é uma tecnologia de comunicação sem fio desenvolvida pela empresa de telecomunicações Ericsson, em 1994. Permite a troca de dados e arquivos entre celulares, computadores, scanners, fones de ouvido e demais disposi vos de forma rápida e segura.

[2] Cartão de segurança: é um recurso u lizado para fornecer aos usuários de internet banking mais segurança na realização de transações financeiras. Ao realizar transações financeiras como pagamentos e transferências, o internet banking solicitará ao usuário que informe uma das contra senhas con das no cartão.

[3] Cer ficação digital: é a tecnologia que por meio da criptografia de dados garante auten cidade, confidencialidade, integridade e não-repúdio às informações eletrônicas.

[4] Check-in: é um recurso na qual é possível marcar onde você está e publicar para os seus amigos nas redes sociais.

[5] Código malicioso: ou Malware (Malicious So ware) é um termo genérico que abrange todos os pos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.

[6] Crimes ciberné cos: são a vidades ilegais pra cadas em ambiente virtual que vão além do roubo de informações financeiras. U lizam-se de computadores e internet para a ngir os mais variados obje vos, seja por meio de uma rede pública, privada ou domés ca.

[7] Criptografia: é a prá ca de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam

ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica.

[8] Firewall: são programas de segurança que fazem a checagem das informações vindas da Internet e ajudam a

impedir que malware, worm e hackers obtenham acesso ao seu computador. Eles filtram o fluxo de dados entre a máquina e uma rede, permi ndo o acesso somente de so wares confiáveis.

[9] HTML: é a sigla de HyperText Markup Language, expressão inglesa que significa "Linguagem de Marcação de Hipertexto". Consiste em uma linguagem de marcação u lizada para produção de páginas na web, que permite a criação de documentos que podem ser lidos em pra camente qualquer po de computador e transmi dos pela internet.

[10] HTTP: significa HyperText Transfer Protocol que em português significa "Protocolo de Transferência de Hipertexto". É um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na World Wide Web (Internet).

[11] HTTPS: Hyper Text Transfer Protocol Secure, que em português significa “Protocolo de Transferência de Hipertexto Seguro”. mais segura do protocolo de transferência de dados entre redes de computadores na internet, pois faz a encriptação dos dados fornecidos, requer a auten cação dos servidores, entre outras ferramentas que garantam a segurança dos dados enviados e recebidos pelo usuário.

[12] Java Script: é uma linguagem de programação baseada em scripts e padronizada pela ECMA Interna onal (associação especializada na padronização de sistemas de informação).

[13] Logs: é uma expressão u lizada para descrever o processo de registro de eventos relevantes num sistema

computacional. Esse registro pode ser u lizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado.

[14] P2P: Peer-to-peer (do inglês par-a-par ou simplesmente ponto-a-ponto) é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permi ndo compar lhamentos de serviços e dados sem a necessidade de um

servidor central.

28

[15] URL: é o endereço de um recurso disponível em uma rede, seja a rede internet ou intranet, e significa em inglês Uniform Resource Locator, e em português é conhecido por Localizador Padrão de Recursos. Em outras palavras, url é um endereço virtual com um caminho que indica onde está o que o usuário procura, e pode ser tanto um arquivo, como uma máquina, uma página, um site, uma pasta etc. Url também pode ser o link ou endereço de um site.

[16] Verificação em duas etapas: é um mecanismo de segurança feito para impedir o acesso não autorizado a contas mesmo quando a senha é comprome da. Com ela, o usuário possui uma senha temporária para verificar a sua iden dade, que é criada temporariamente e u lizada uma única vez.

Em geral, esse código é distribuído das seguintes formas: envio de um SMS, criação de um código por meio de um aplica vo mobile ou u lização de um token sico conectado via USB ou por meio da tecnologia NFC.

[17] VPN: (Virtual private network – rede virtual privada) é uma ferramenta que permite o tráfego de dados por um caminho priva vo na web. Na navegação comum, por exemplo, quando um endereço de site está com o início “h ps://”, em vez de “h p://”, significa que esta é uma conexão segura, na qual se estabelece uma VPN entre o seu computador e o servidor do site que você está acessando. Existem outras aplicações para a VPN.

Document Outline

Document Outline