CYBER SAFE

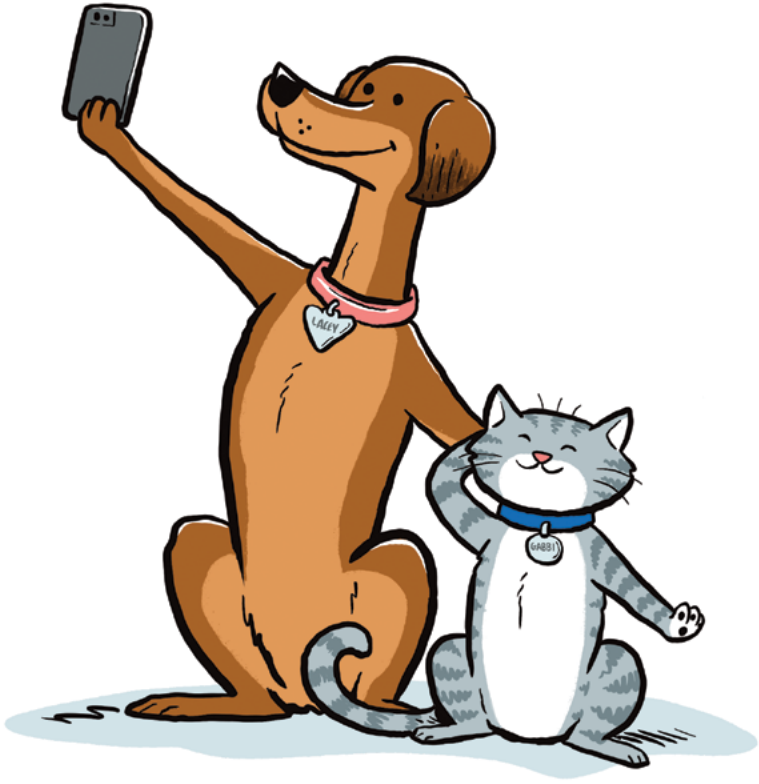
Dicas de uma cachorrinha para segurança na Internet

Renee Tarun & Susan Burg

FORTINET

CYBER SAFE

Dicas de uma cachorrinha para segurança na Internet



Por Renee Tarun e Susan Burg

Ilustrações: Terry LaBan

FORTINET®

ÍNDICE

O que é Internet?..... 4

O que você pode fazer na Internet?..... 5

Por que Cibersegurança?..... 6

Senhas: Tranque a porta..... 8

Atualizações e Antivírus..... 10

Não clique: Proteja-se do "phishing"..... 11

Não fale com estranhos..... 12

Como se manter seguro..... 13

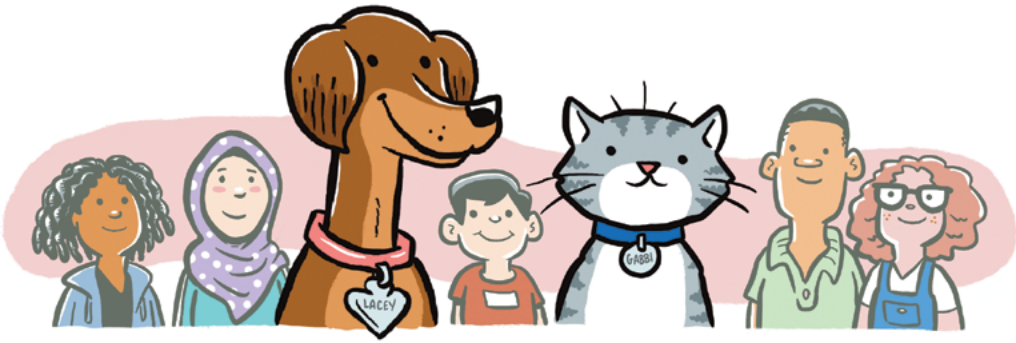
Postando nas redes..... 14

Sendo um bom camarada..... 15

Glossário..... 16

Lembre-se de P.A.T.A. para ficar seguro..... 17

Guia para os pais..... 18



Para meus filhos, Ryan e Becca – Eu amo vocês e espero que vocês estejam sempre seguros

Para Brett – Obrigada por sempre ser a minha luz

-Renee Tarun

Aos meus alunos de todas as idades:
Estejam seguros on-line e façam boas escolhas.
Eu quero que um dia vocês digam: "A sra. Burg me ensinou muito...
assim como a cachorrinha e o gato do livro Cyber Safe."

-Susan Burg

Fortinet
899 Kifer Rd.
Sunnyvale, CA 94086

Tradução: Marina Wodewotzky

Primeira edição

Sobre os autores

Renee Tarun é uma mãe com mais de 20 anos de experiência em segurança cibernética. Ela é vice Chief Information Security Officer (CISO) na Fortinet; antes disso, trabalhou na Agência de Segurança Nacional (NSA) dos Estados Unidos.

Susan Burg é professora certificada pelo Conselho Nacional dos EUA, com 24 anos de experiência em ensino. Ela adora crianças e adora escrever; atualmente, ela está trabalhando em uma série de livros infantis sobre uma garotinha chamada Gracie.

Renee e Susan são boas amigas que compartilham a paixão por manter as crianças seguras on-line. Os personagens do livro foram inspirados em seus animais de estimação, Lacey e Gabbi, que trouxeram muita alegria e felicidade para suas famílias. Eles deixarão suas patinhas marcadas em nossos corações para sempre.

Agradecimentos

Queremos agradecer à Fortinet por apoiar este livro e por seu profundo compromisso com a segurança cibernética de crianças e adultos.


Olha, Gabbi! É uma armadilha!
O que há de errado, Lacey? Você não quer brinquedos grátis?
BRINQUEDOS GRÁTIS PARA PETS
CLIQUE AQUI


O que eles realmente querem são minhas informações pessoais!
Eles sabem que você é uma cadela?
BRINQUEDOS GRÁTIS PARA PETS
CLIQUE AQUI
Na Internet, ninguém sabe que eu sou uma cadela. E eu também não sei quem eles são!
E isso é ruim?
LACEY
GABBY
Pode ser. Mamãe e papai estão sempre preocupados com as crianças.
Ah, as crianças apenas jogam e assistem a coisas bobas.
Sim, vídeos de gatos!
Sério, você tem que se proteger!
LACEY
Como algo ruim pode acontecer se eu nem estou saindo do sofá?
Vamos falar sobre isso!

O QUE É INTERNET?

Muitas coisas inusitadas estão conectadas à Internet!

OUTRAS FORMAS DE ACESSAR A INTERNET

O QUE VOCÊ PODE FAZER NA INTERNET?

Assistir a vídeos

Conversar com amigos e familiares

Pesquisar e explorar

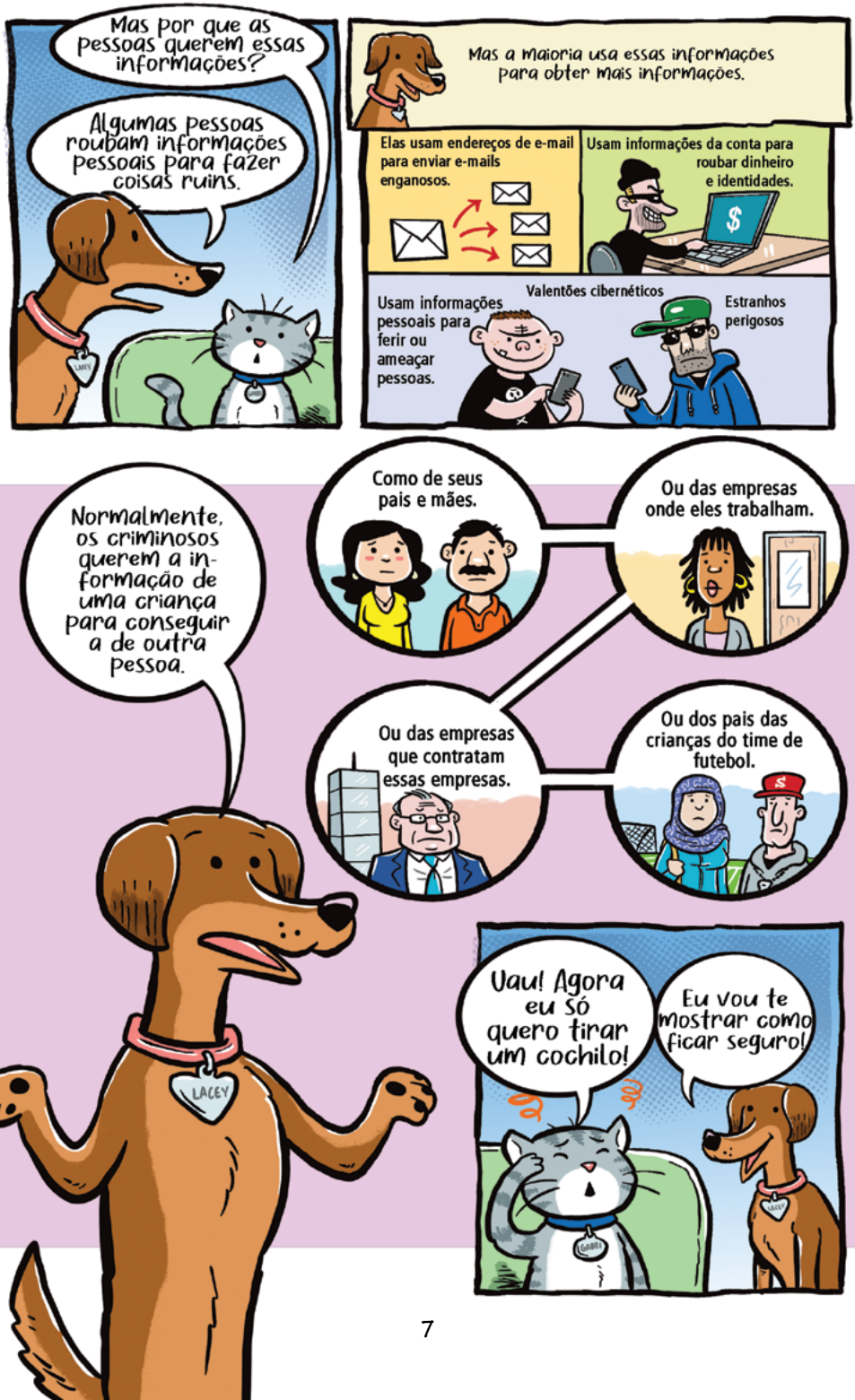
Ouvir música

Aprender quase tudo

Jogar

Descobrir o que está acontecendo

POR QUE CIBERSEGURANÇA?


Mas por que as pessoas querem essas informações?
Algumas pessoas roubam informações pessoais para fazer coisas ruins.
Mas a maioria usa essas informações para obter mais informações.
Elas usam endereços de e-mail para enviar e-mails enganosos.
Usam informações da conta para roubar dinheiro e identidades.
Valentões cibernéticos
Usam informações pessoais para ferir ou ameaçar pessoas.
Estranhos perigosos
Normalmente, os criminosos querem a informação de uma criança para conseguir a de outra pessoa.
Como de seus pais e mães.
Ou das empresas onde eles trabalham.
Ou das empresas que contratam essas empresas.
Ou dos pais das crianças do time de futebol.
LACEY
Uau! Agora eu só quero tirar um cochilo!
Eu vou te mostrar como ficar seguro!

SENHA: TRANQUE A PORTA!

Você sabia? A maioria dos criminosos usa senhas roubadas ou fracas para invadir a conta das pessoas.

REGRAS DA *Senha*

ESCOLHA UMA SENHA QUE SÓ VOCÊ SAIBA

Não use seus dados pessoais – aniversário, endereço, idade ou telefone.

FAÇA COM QUE SEJA DIFÍCIL DE ADIVINHAR

Use letras maiúsculas e minúsculas, números e caracteres especiais como $, # e %

MANTENHA EM SEGREDO

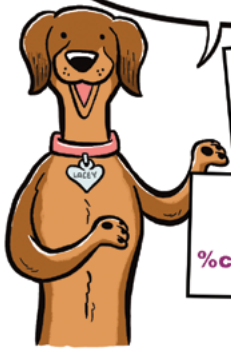
SE ALGO NOVO JÁ VEM COM SENHA, TROQUE-A

NÃO USE SENHAS COMUNS (E RUINS)

Segredo | Futebol | Senha | 1234567 | ABCDE

TAMBÉM É RUIM Usar números como letras **P3RR0**

E não use os seus atores, jogadores ou personagens preferidos!



RUIM
cachorropeludo82

MELHOR
%cACHorrOpe!uDo#82!

Sempre use um código para bloquear tablets e celulares.

ATUALIZAÇÕES E ANTIVÍRUS

TENHA CUIDADO COM:

JOGOS GRÁTIS

Pode conter malware ou pedir seus dados pessoais.

MÚSICA GRÁTIS

Grátis por pouco tempo e então seus pais terão que pagar.

COISAS GRÁTIS

Normalmente são armadilhas para coletar informações.

CONCURSOS

A maioria é falsa – ninguém ganha e os prêmios não existem.

FILIAÇÕES

Clubes são divertidos, mas custam caro.

NÃO CLIQUE!

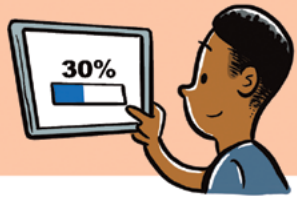
PROTEJA-SE DO PHISHING

Somente abra e-mails de pessoas que você conheça.

Se algo parecer errado, pergunte à pessoa se ela realmente te enviou aquilo.

Não clique em links.

Antes de abrir um anexo (como uma foto ou um vídeo), passe o antivírus.



Você sabia? Phishing significa induzir alguém a clicar em um link que causa algo ruim.

NÃO FALE COM ESTRANHOS

Alguns estranhos fingem ser crianças. Estranhos on-line podem ser tão perigosos quanto estranhos na vida real.

ESTRANHOS PERIGOSOS!

PERGUNTE-SE:

COMO SE MANTER SEGURO

Converse apenas com pessoas que você conheça na vida real.

Não compartilhe informações pessoais on-line.

Não confie em estranhos, nem dê ouvidos a eles.

Nunca encontre com estranhos pessoalmente.

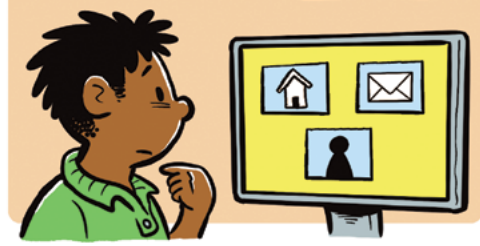
Não siga um estranho de um aplicativo para outro.

Se um estranho disser para não contar, você definitivamente tem que contar.

Se algo parecer estranho on-line, fale com um adulto de confiança.

POSTANDO NAS REDES

Proteja todas as suas informações. Nunca forneça seu nome, número de telefone, e-mail, senha, endereço, nome da escola ou sua foto sem a permissão dos seus pais.



Mostre a um adulto de confiança antes de postar qualquer coisa on-line.

SENDO UM BOM CAMARADA

CYBERBULLYING É UM GRANDE PROBLEMA

É o mesmo que ofender pessoalmente, mas o agressor se esconde atrás de um teclado.

Algumas pessoas dizem coisas on-line que não diriam na sua cara.

O cyberbullying machuca!

O QUE AS CRIANÇAS PODEM FAZER

Não responda a postagens maliciosas ou ofensivas.

Conte a seus pais ou a um professor se você presenciar cyberbullying.

Seja educado e respeitoso com todos.

Atualizações
Os recursos e correções mais recentes para computadores, dispositivos e aplicativos. Frequentemente inclui correções para problemas de segurança.

Antivírus
Software que protege computadores e dispositivos contra vírus e malware.

Ciberespaço
Outro nome para a Internet.

Cibersegurança
Práticas para se manter seguro on-line.

Clique
Para selecionar algo em uma tela, seja por toque, mouse, teclado ou comando de voz.

Código de acesso
Um código ou senha que desbloqueia um dispositivo como um telefone ou tablet.

Correio eletrônico em massa
Lixo eletrônico enviado para muitas pessoas. Pode conter vírus ou golpes cibernéticos. Também é conhecido como spam.

Cyberbullying
Ser maldoso com outra pessoa na Internet.

Dados pessoais
Informações como seu número de telefone, aniversário, endereço e assim por diante.

Em linha (on-line)
Acessar a Internet.

Estranho
Alguém que você não conhece.

Informações pessoais
Inclui todos os detalhes sobre você, como idade, nome, endereço, cor do cabelo, aniversário, escola, série, time de futebol, cidade natal e muito mais.

Internet
Uma rede mundial de computadores interconectados.

Malware
É um software malicioso (mau). Malware inclui adware (propaganda indesejada), vírus, spyware (software de espionagem), worms (malware que se multiplica sozinho) e muito mais.

Senha
Uma sequência secreta de letras, números e caracteres que permite acessar softwares ou sites.

Phishing
Uma tentativa de coletar informações pessoais por meio de e-mails, mensagens ou site enganosos.

Postar
Colocar qualquer coisa on-line (palavras, imagens, vídeos).

Wi-Fi público
Wi-Fi disponível em locais públicos que não são criptografados (codificados para privacidade).

Vírus
Um vírus de computador é um programa projetado para se espalhar para outros computadores, tornando-os vulneráveis a ataques.

Lembre-se de P. A. T. A. para ficar seguro

PROTEJA

Suas informações pessoais e não poste sem a permissão de seus pais.

ATENÇÃO

Diante de qualquer convite de pessoas desconhecidas. Nunca encontre estranhos pessoalmente.

TODA VEZ

Que vir qualquer coisa triste, desconfortável ou confusa, converse com um adulto de confiança.

ATUE

De forma positiva e não responda a mensagens maldosas ou ofensivas.

GUIA

Converse com seus filhos

Considere estabelecer limites:

- Defina quanto tempo as crianças podem ficar on-line.
- Diga a eles quais sites eles têm permissão para visitar.
- Especifique o software/aplicativo que eles podem usar.
- Permita atividades ou tarefas adequadas à idade, com base no conhecimento e maturidade deles.

Priorize a privacidade

Publicar informações pessoais ou fotos na Internet pode ser perigoso, pois há pessoas que podem utilizá-las de forma prejudicial.

- Fotos e informações pessoais compartilhadas podem causar problemas mais tarde.
- É difícil remover qualquer coisa on-line, uma vez que caia no domínio público.
- Verifique as configurações de privacidade nas redes sociais para evitar que estranhos acessem informações pessoais. As configurações predefinidas podem não ser as ideais.

Explique os quatro "nãos":

- Não forneça seu nome, número de telefone, e-mail, senha, endereço, escola ou foto sem permissão dos pais.
- Não responda a postagens maliciosas ou prejudiciais.
- Não abra e-mails ou anexos de pessoas que você não conheça.
- Não encontre pessoalmente com ninguém que você "conheceu" on-line.

Se viu algo, diga algo

- Converse com seus filhos sobre os perigos da Internet para que eles reconheçam comportamentos ou atividades suspeitas.
- Deixe claro aos seus filhos que, se eles virem algo em um site, e-mail ou bate-papo que não pareça correto ou os deixe desconfortáveis, eles podem vir até você com suas perguntas e preocupações.

PARA OS PAIS

Mantenha tudo atualizado

- Os pais devem instalar todas as atualizações em seus dispositivos e aplicativos.
- Os pais devem instalar e executar um antivírus.

Esteja atento e sempre presente

- Saiba o que seu filho está fazendo na Internet, incluindo os sites que ele está visitando.
- Se eles estiverem usando e-mail, mensagens instantâneas ou salas de bate-papo, certifique-se de saber com quem eles estão se comunicando.
- Certifique-se de que seu filho realmente conhece as pessoas com quem está falando on-line.

Mantenha os computadores acessíveis

- Se o seu computador estiver em uma área comum, você pode monitorar facilmente sua atividade.
- Se as crianças perceberem que você pode ver a tela, isso ajudará a evitar que elas façam coisas que não deveriam.
- A visibilidade dá a você a oportunidade de intervir se notar um comportamento que pode ter consequências negativas.

Pergunte ao seu provedor de Internet sobre o controle parental

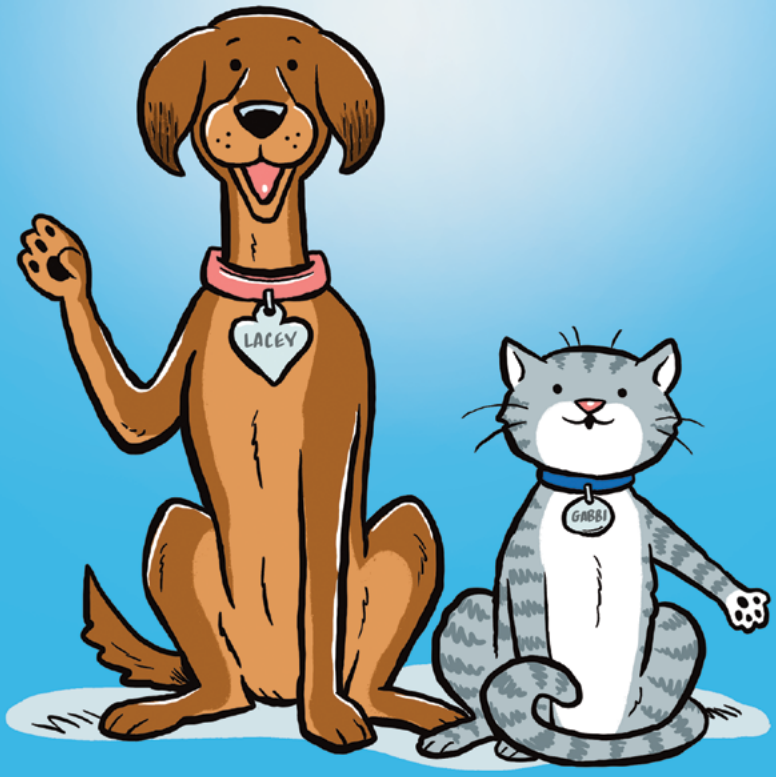
Alguns provedores de Internet oferecem serviços (às vezes gratuitos) projetados, especificamente, para proteger as crianças on-line, restringindo o acesso a sites ou a recursos de comunicação como e-mail, bate-papo e mensagens instantâneas por idade, conteúdo, horário e outras categorias. Entre em contato com seu provedor para descobrir os serviços disponíveis.

Proteção adicional

Alguns navegadores permitem que você restrinja ou permita apenas determinados sites e você pode proteger essas configurações com uma senha. Embora nenhuma tecnologia seja infalível, considere o uso de aplicativos que ofereçam essa proteção adicional, monitorando, filtrando e restringindo o acesso a conteúdos perigosos.

Todo mundo diz que você deve ter cuidado on-line. Mas o que isso significa?

Lacey é uma cachorrinha muito inteligente que protege as crianças ensinando-as como se manterem seguras on-line. Junte-se à Lacey e ao seu amigo Gabbi em uma divertida aventura cibernética e aprenda como agir e como se manter seguro on-line.



ISBN: 978-1-09835-735-1

9 781098 357351

FORTINET