An Elected Office of
RAMSEY COUNTY

Ramsey County Sheriff’s Office

Jack Serier, Sheriff

Cyber Safety

How secure is your online life?

Crime Prevention Unit

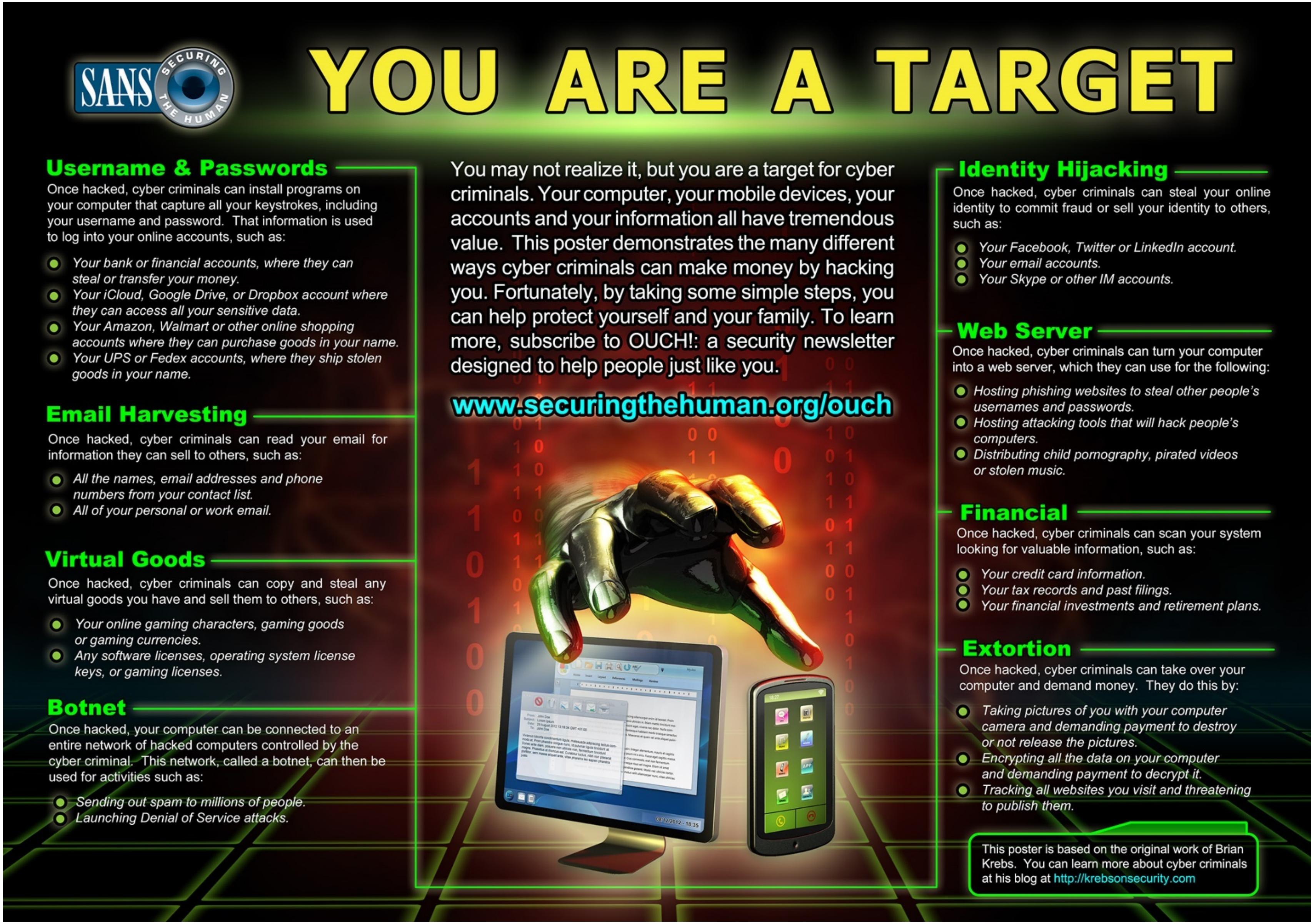
Today’s world is interconnected

Yet, for all its advantages, increased connectivity brings increased risk of theft, fraud, and abuse.

Cyber Safety is always a concern

Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment.

Every time we connect to the Internet—at home, at school, at work, or on our mobile devices—we make decisions that affect our cybersecurity



YOU ARE A TARGET

SANS SECURING THE HUMAN

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

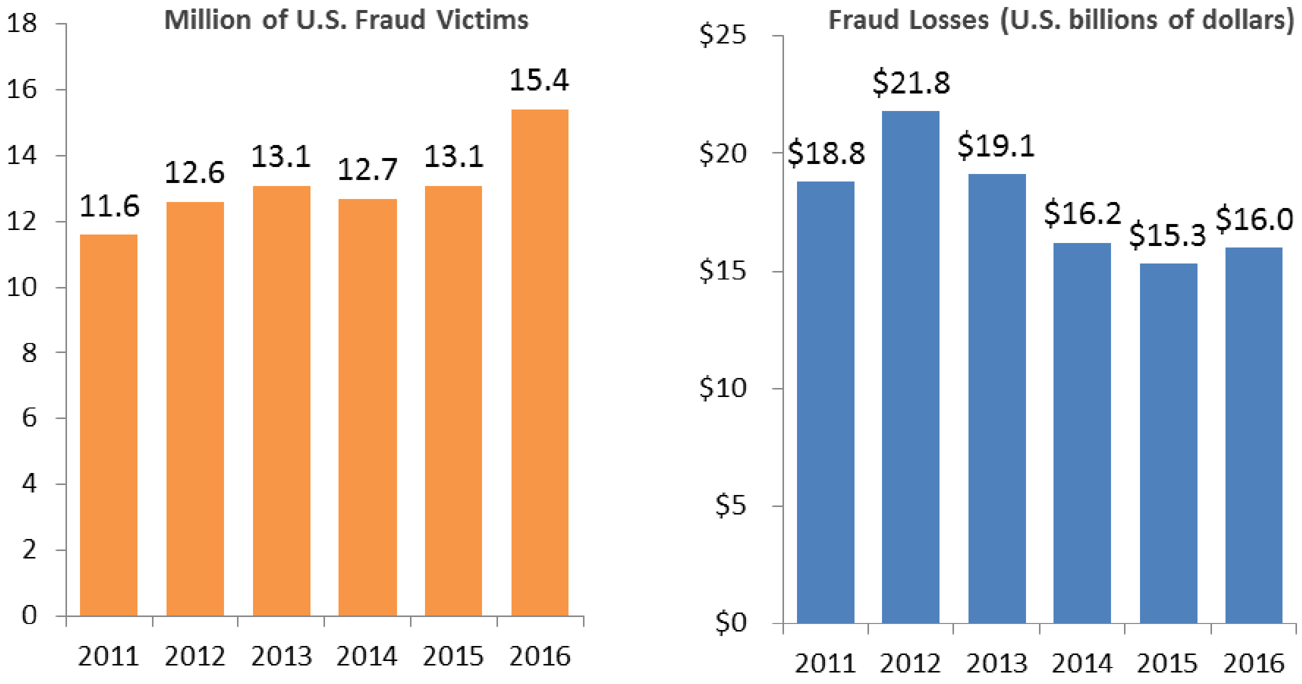
Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com

Identity Theft – Billions in losses

Total Fraud Victims Reaches Record High



Source: *2017 Identity Fraud Study*, Javelin Strategy & Research.

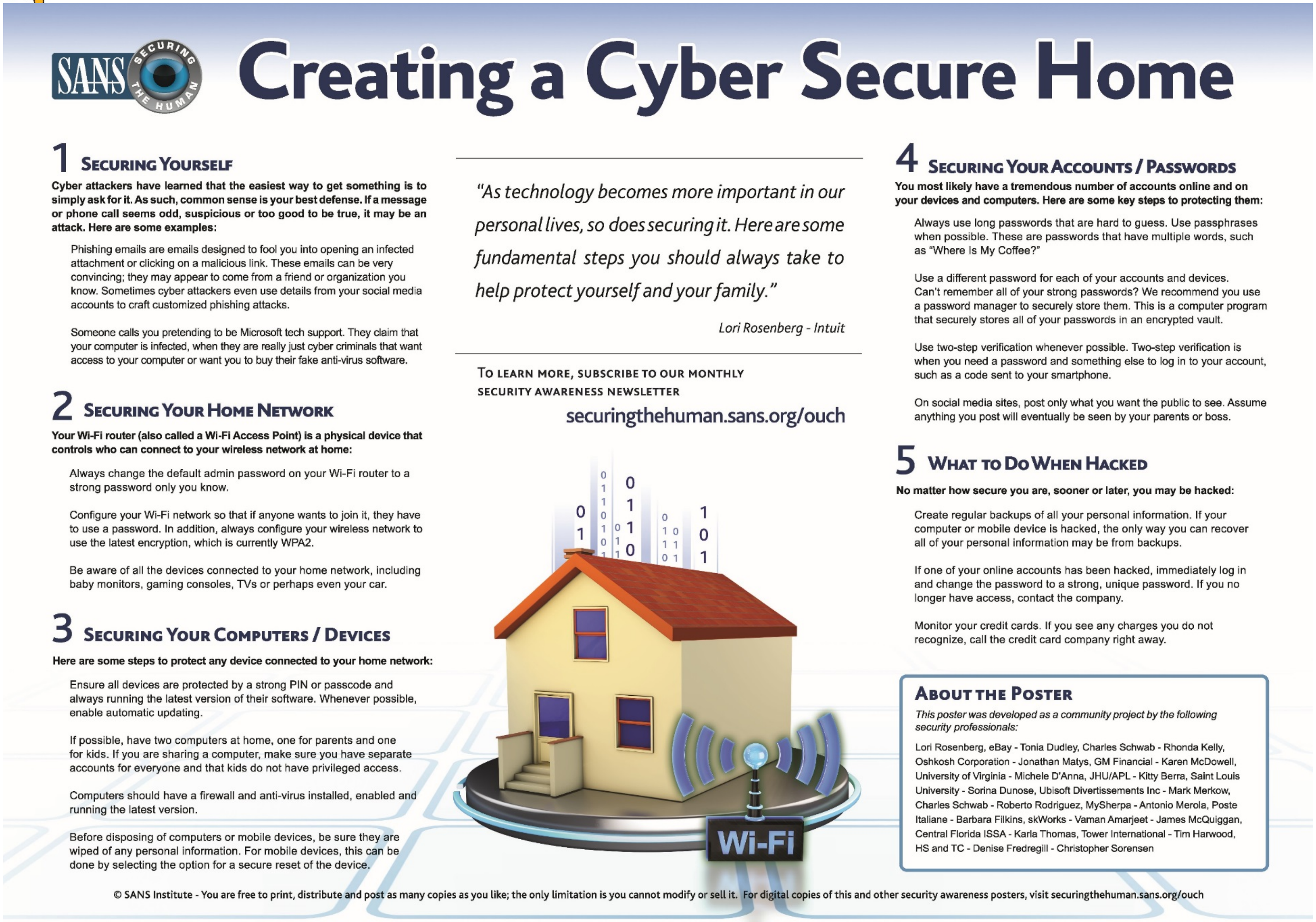
JAVELIN

Four significant trends found in 2016 fraud

- **Fraud leaps to record high incidence** – in 2016 6.1% of consumers became victims of identity fraud, an increase of more than 2 million victims
- **Card-not-present (CNP) fraud rose significantly** – with the growth of e-commerce fraudsters moved online, increasing CNP fraud by 40%
- **Account takeover losses high** - $2.3 billion in 2016, a 61% increase from 2015, while incidence rose 31%
- **New-account fraud continues unabated** – fraudsters have become better at evading detection, with victims likely to discover fraud through review of credit report (15%) or when contacted by a debt collector (13%)

How It's Done

- Thieves obtain personal information about victims
- Use information to access existing or create new accounts
- Spend money as fast as they can
- Move on to the next victim



Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

> *"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."*
>
> *Lori Rosenberg - Intuit*

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where Is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

About the Poster

This poster was developed as a community project by the following security professionals:

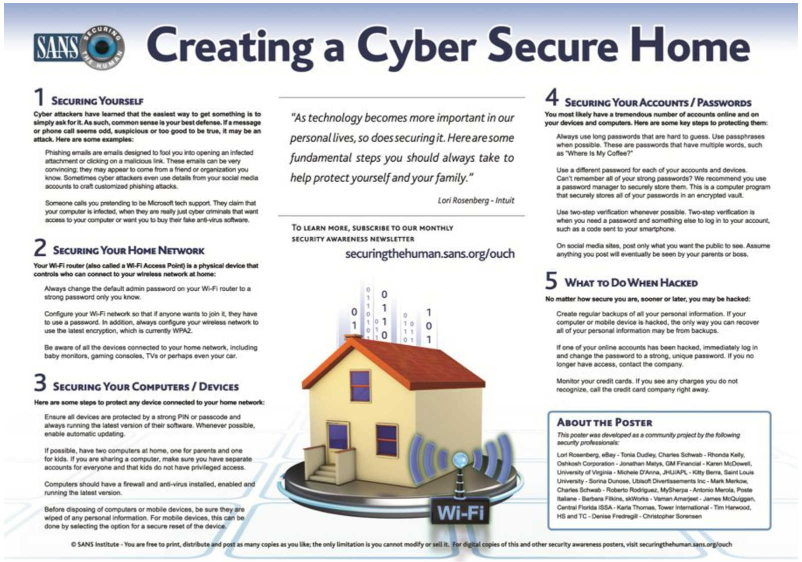
Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Matys, GM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berra, Saint Louis University - Sorina Dunose, Ubisoft Divertissements Inc - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, skWorks - Vaman Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

Securing Yourself

Cyber attackers have learned that the easiest way to get something is to ask for it.

Common sense is your best defense.

If a message or phone call seems odd, suspicious or too good to be true, it may be an attack.



Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - Intuit

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where Is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

About the Poster

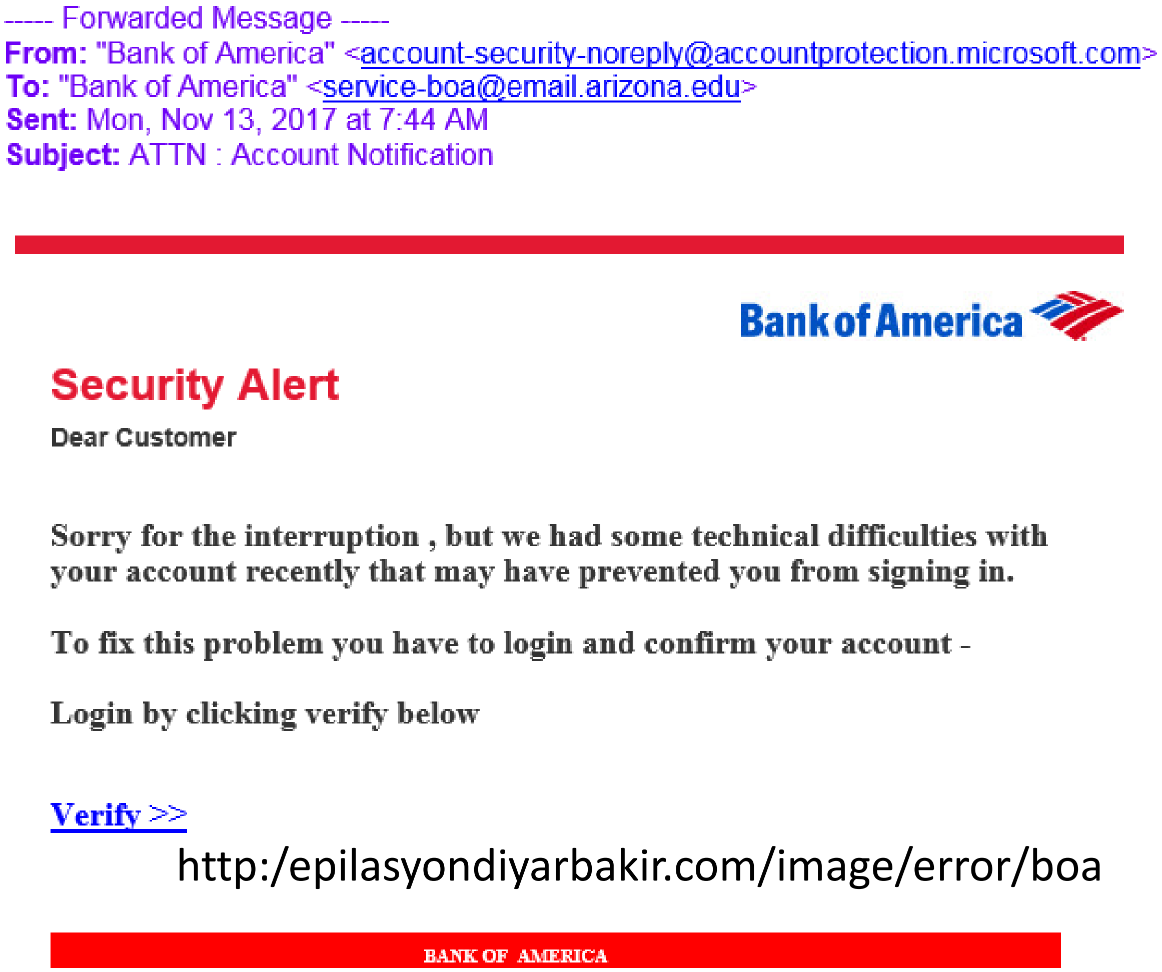
This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Matys, GM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berra, Saint Louis University - Sorina Dunose, Ubisoft Divertissements Inc - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, skWorks - Vaman Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link.

They can be very convincing, appearing to come from an organization or person you know. Sometimes cyber attackers even use details from your social media account to craft customized phishing attacks.

Email – phishing for your information



----- Forwarded Message -----
From: "Bank of America" <account-security-noreply@accountprotection.microsoft.com>
To: "Bank of America" <service-boa@email.arizona.edu>
Sent: Mon, Nov 13, 2017 at 7:44 AM
Subject: ATTN : Account Notification

Bank of America

Security Alert

Dear Customer

Sorry for the interruption , but we had some technical difficulties with your account recently that may have prevented you from signing in.

To fix this problem you have to login and confirm your account -

Login by clicking verify below

Verify >>

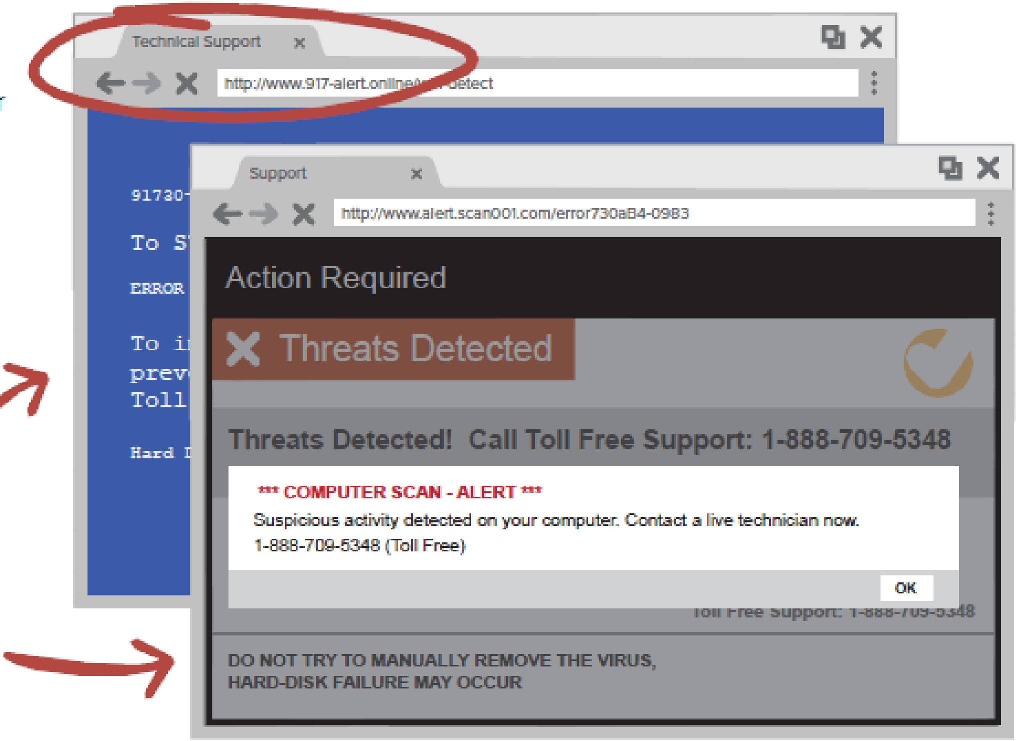
http:/epilasyondiyarbakir.com/image/error/boa

BANK OF AMERICA

Spotting a Tech Support Scam

It often starts with a pop-up . . .

Shows up within your **internet browser**



Threats Detected! Call Toll Free Support: 1-888-709-5348

*** COMPUTER SCAN - ALERT ***

Suspicious activity detected on your computer. Contact a live technician now.

1-888-709-5348 (Toll Free)

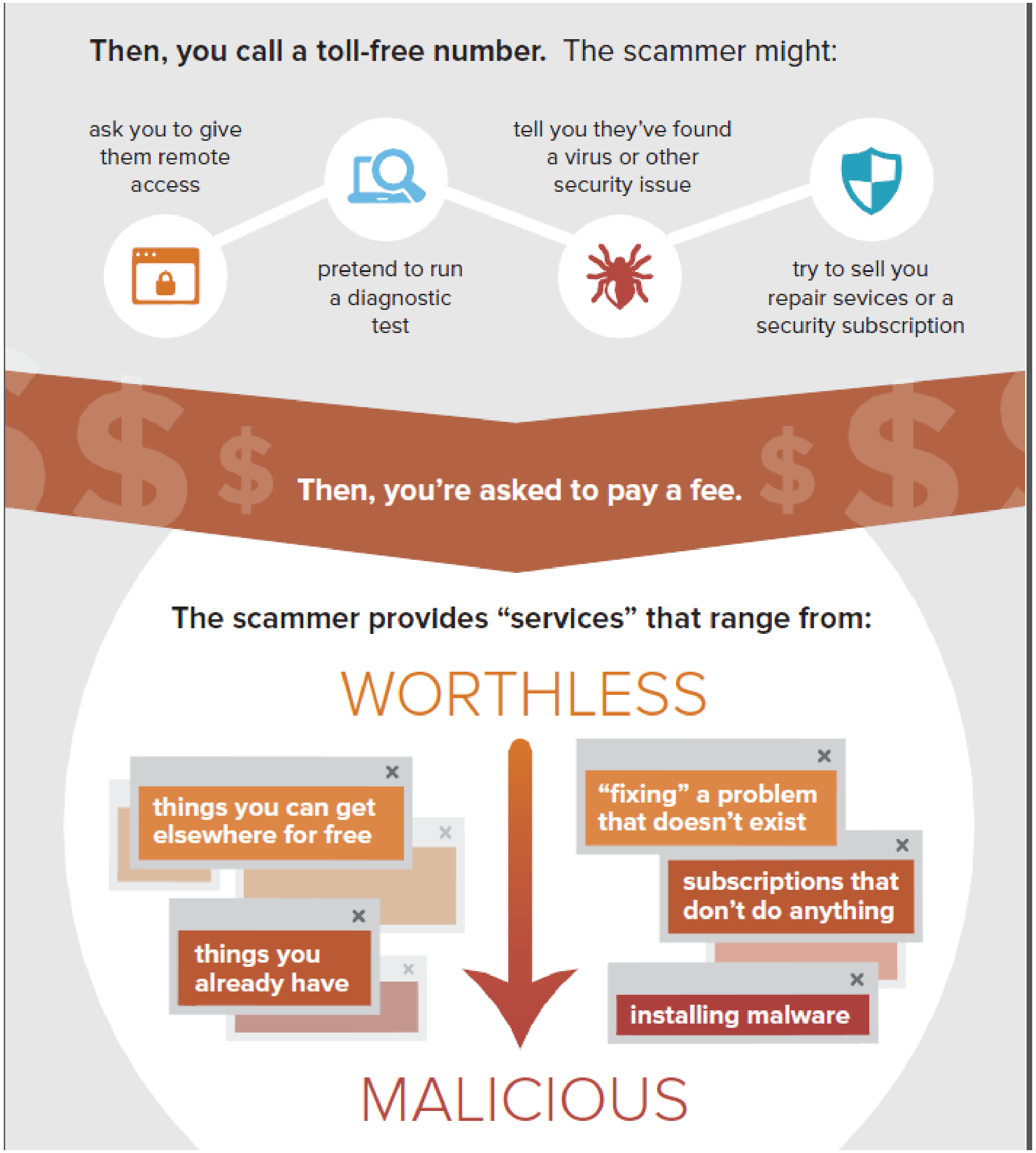
Toll Free Support: 1-888-709-5348

DO NOT TRY TO MANUALLY REMOVE THE VIRUS,
HARD-DISK FAILURE MAY OCCUR

Might **imitate** a blue error screen

or trusted antivirus software

CALL	NOW	OR ELSE...
Wants you to call a **toll-free number**	Urges you to call **immediately**	Threatens that you may **lose personal data** if you don't call



Then, you call a toll-free number. The scammer might:

ask you to give them remote access

pretend to run a diagnostic test

tell you they've found a virus or other security issue

try to sell you repair sevices or a security subscription

Then, you're asked to pay a fee.

The scammer provides "services" that range from:

WORTHLESS

things you can get elsewhere for free

things you already have

"fixing" a problem that doesn't exist

subscriptions that don't do anything

installing malware

MALICIOUS

WHAT YOU CAN DO:

→ If you get a pop-up, call, spam email or any other urgent message about a virus on your computer, **stop**.

Don't click on any links or call a phone number.

Don't send any money.

Don't give anyone control of your computer.

Microsoft does not display pop-up warnings and ask you to call a toll-free number about viruses or security problems.

→ **Report it** at ftc.gov/complaint. Include the phone number that you were told to call.

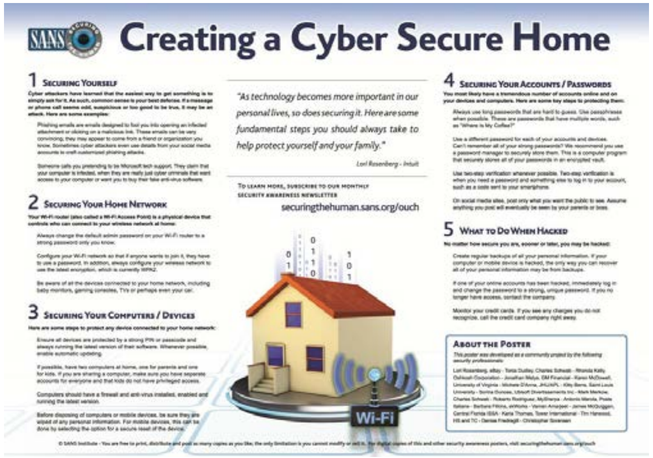
→ Keep **your security software** up to date. Know what it looks like so you can spot a fake.

→ **Tell someone** about this scam. You might help them spot it and avoid a costly call.

LEARN MORE: ftc.gov/TechSupportScams

Securing Your Home Network

Your Wi-Fi router is a physical device that controls who can connect to your wireless network at home.



Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing, they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - Intuit

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

About the Poster

This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Melys, DM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berns, Saint Louis University - Sorina Duncea, Ubisoft Divertissements Inc. - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, eWorks - Varnan Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

© SANS Institute - You are free to print, distribute and post as many copies as you like, the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit securingthehuman.sans.org/ouch

Always change the default admin password to a strong password you know.

Configure your network to require a password for those that connect. Use the latest encryption (currently WPA2).

Be aware of all devices connected to your home network, including baby monitors, gaming consoles, TVs, or perhaps your car.

SANS

Creating a Cyber Secure Home

1 Securing Yourself

[illegible]

2 Securing Your Home Network

[illegible]

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - Intuit

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch

4 Securing Your Accounts / Passwords

[illegible]

5 What to Do When Hacked

[illegible]

About the Poster

[illegible]

[illegible]

Securing Your Computers / Devices

Ensure all devices are protected by a strong PIN or passcode and are running the latest version of their software.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer make sure you have separate accounts for everyone and that kids do not have privileged access.

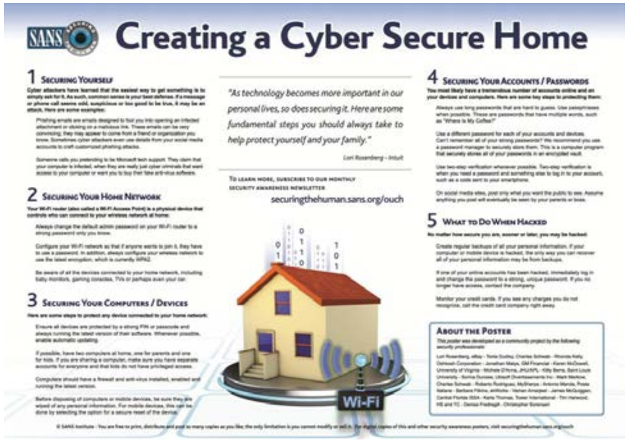
Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information.

Securing Your Accounts / Passwords

Managing those numerous online accounts, devices and computers.

Tips from a college poster:



SANS Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home.

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - Intuit

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked.

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

About the Poster

This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay · Tonia Dudley, Charles Schwab · Rhonda Kelly, Oshkosh Corporation · Jonathan Matys, GM Financial · Karen McDowell, University of Virginia · Michele D'Anna, JHU/APL · Kitty Berra, Saint Louis University · Sonia Dunseo, Ubisoft Divertissements Inc · Mark Merkow, Charles Schwab · Roberto Rodriguez, MyShenpa · Antonio Merola, Poste Italiane · Barbara Filkins, sinfonia · Vernon Amarjeet · James McQuiggan, Central Florida ISSA · Karla Thomas, Tower International · Tim Harwood, HS and TC · Denise Fredregill · Christopher Sorensen

© SANS Institute - You are free to print, distribute and post as many copies as you like; the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit securingthehuman.sans.org/ouch

Use strong passwords

My passwords are long, complex, and don't contain dictionary words

I never share my passwords

I use different passwords for different services

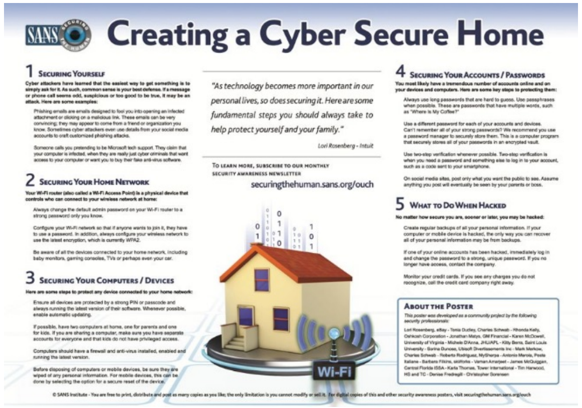
I use different passwords for home and school/work

I store my passwords securely

I use multifactor authentication like Google's 2-step verification

What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked.



SANS SECURING THE HUMAN

Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network

Your Wi-Fi router (also called a Wi-Fi Access Point) is a physical device that controls who can connect to your wireless network at home:

Always change the default admin password on your Wi-Fi router to a strong password only you know.

Configure your Wi-Fi network so that if anyone wants to join it, they have to use a password. In addition, always configure your wireless network to use the latest encryption, which is currently WPA2.

Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs or perhaps even your car.

3 Securing Your Computers / Devices

Here are some steps to protect any device connected to your home network:

Ensure all devices are protected by a strong PIN or passcode and always running the latest version of their software. Whenever possible, enable automatic updating.

If possible, have two computers at home, one for parents and one for kids. If you are sharing a computer, make sure you have separate accounts for everyone and that kids do not have privileged access.

Computers should have a firewall and anti-virus installed, enabled and running the latest version.

Before disposing of computers or mobile devices, be sure they are wiped of any personal information. For mobile devices, this can be done by selecting the option for a secure reset of the device.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - Intuit

To learn more, subscribe to our monthly security awareness newsletter

securingthehuman.sans.org/ouch

4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as "Where is My Coffee?"

Use a different password for each of your accounts and devices. Can't remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your account, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume anything you post will eventually be seen by your parents or boss.

5 What to Do When Hacked

No matter how secure you are, sooner or later, you may be hacked:

Create regular backups of all your personal information. If your computer or mobile device is hacked, the only way you can recover all of your personal information may be from backups.

If one of your online accounts has been hacked, immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

About the Poster

This poster was developed as a community project by the following security professionals:

Lori Rosenberg, eBay - Tonia Dudley, Charles Schwab - Rhonda Kelly, Oshkosh Corporation - Jonathan Matys, GM Financial - Karen McDowell, University of Virginia - Michele D'Anna, JHU/APL - Kitty Berns, Saint Louis University - Sorina Dunose, Ubisoft Divertissements Inc - Mark Merkow, Charles Schwab - Roberto Rodriguez, MySherpa - Antonio Merola, Poste Italiane - Barbara Filkins, skWorks - Vaman Amarjeet - James McQuiggan, Central Florida ISSA - Karla Thomas, Tower International - Tim Harwood, HS and TC - Denise Fredregill - Christopher Sorensen

Create regular backups of all your personal information.

If an online account is hacked immediately log in and change the password to a strong, unique password. If you no longer have access, contact the company.

Monitor your credit cards. If you see any charges you do not recognize, call the credit card company right away.

Protecting our children

- Our children are living in a world with technology far advanced from what we experienced in our youth
- The Internet is a wonderful tool that enables our kids to tap into a vast wealth of knowledge, learn about a variety of topics, build a network of friends, and to interact with people and cultures around the world
- Our job as parents is to educate and mentor them on how to navigate this large and often confusing world safely and securely

3 Dangers kids face online

- **Strangers** – can pretend to be anything they want online. Threats include sexual predators and fraud (game accounts)
- **Friends** – same threats we faced growing up, but on a bigger scale and can happen anonymously. Cyber bullying, pranks, sextortion, ex-boy/girlfriends, etc.
- **Themselves** - can mistakenly believe what they share can be private or can be removed. Sharing too much. Accessing inappropriate content. Spending too much time online. Bullying or harassing others. Damaging their reputation. Downloading or sharing copyrighted material.

Know The Facts:

Become a Cyberaware Parent

RSAC CyberSafety: Kids

One in 25 children ages 10 to 17 received an online sexual solicitation where the solicitor tried to make offline contact.[1]

NEARLY 50% of children in kindergarten or 1st grade report interacting with people on web sites. **Only half have parents who watch their activity while they use a computer.**[2]

ABOUT 11% **of teens report knowing how to turn off parental controls,** which you can use to block certain types of Web content.[3]

38% **of kids under age 2 have used a mobile device.** Three fourths of all kids have access to mobile devices at home.[4]

Studies say that almost half of kids between ages 10 and 17 are consuming porn online— **and close to one third of teens are sending their own nude photos.**[5]

Nearly **one in 10 teens** has posted his or her cell phone number online.[6]

Are these stats startling to you?
Pledge to keep your kids cybersafe
by joining the RSAC CyberSafety: Kids initiative:
http://www.rsaconference.com/about/rsac-cyber-safety/im-in-ru

SOURCES

[1] https://www.nsopw.gov/en/Education/FactsStatistics?AspxAutoDetectCookieSupport=1

[2] http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=2426&context=article

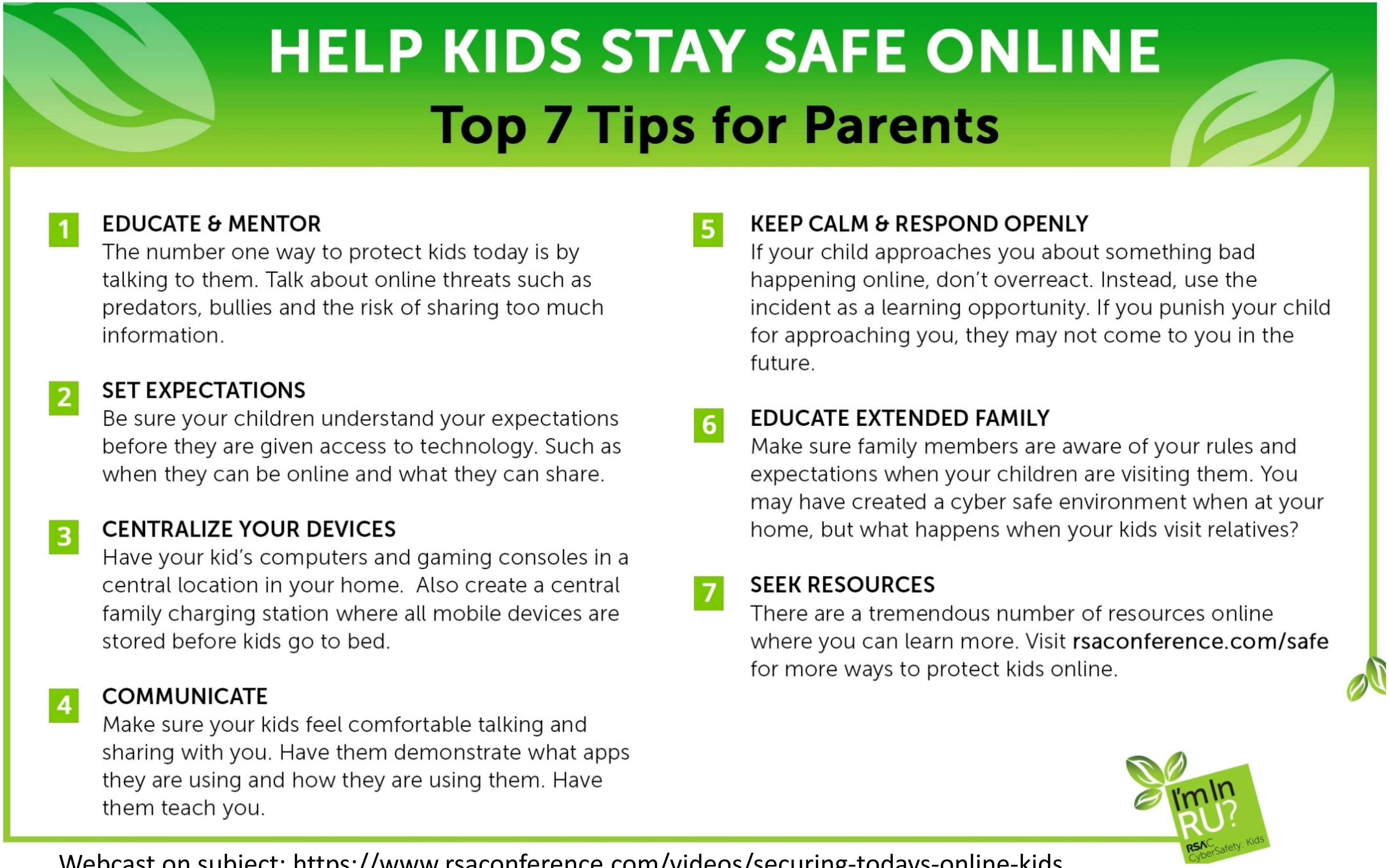
[3] http://safekids.com/mcafee_harris.pdf

[4] https://www.commonsensemedia.org/research/zero-to-eight-childrens-media-use-in-america-2013

[5] http://pediatrics.aappublications.org/content/119/2/247.abstract

[6] http://www.cox.com/wcm/en/aboutus/datasheet/takecharge/archives/2007-teen-survey.pdf?campcode=takecharge-archive-link_2007-survey_0511

RSAConference2016



HELP KIDS STAY SAFE ONLINE

Top 7 Tips for Parents

1 EDUCATE & MENTOR
The number one way to protect kids today is by talking to them. Talk about online threats such as predators, bullies and the risk of sharing too much information.

2 SET EXPECTATIONS
Be sure your children understand your expectations before they are given access to technology. Such as when they can be online and what they can share.

3 CENTRALIZE YOUR DEVICES
Have your kid's computers and gaming consoles in a central location in your home. Also create a central family charging station where all mobile devices are stored before kids go to bed.

4 COMMUNICATE
Make sure your kids feel comfortable talking and sharing with you. Have them demonstrate what apps they are using and how they are using them. Have them teach you.

5 KEEP CALM & RESPOND OPENLY
If your child approaches you about something bad happening online, don't overreact. Instead, use the incident as a learning opportunity. If you punish your child for approaching you, they may not come to you in the future.

6 EDUCATE EXTENDED FAMILY
Make sure family members are aware of your rules and expectations when your children are visiting them. You may have created a cyber safe environment when at your home, but what happens when your kids visit relatives?

7 SEEK RESOURCES
There are a tremendous number of resources online where you can learn more. Visit **rsaconference.com/safe** for more ways to protect kids online.

I'm In RU?
RSAC CyberSafety: Kids

Webcast on subject: https://www.rsaconference.com/videos/securing-todays-online-kids

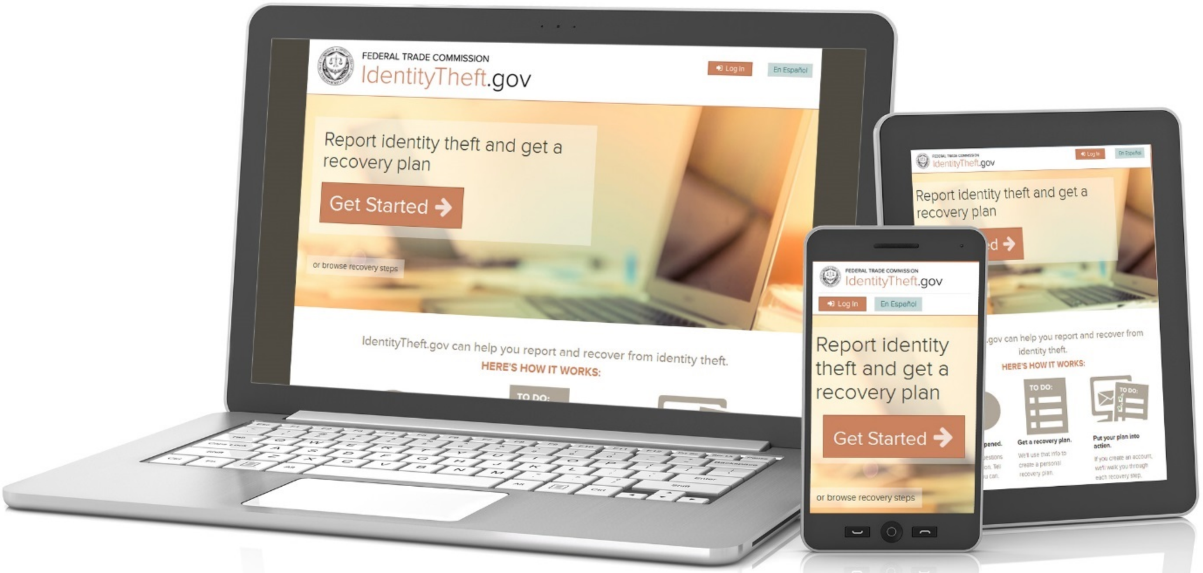
Tips for using Public Wi-Fi Networks

- When using a hotspot, log in or send personal information only to websites you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to one of your accounts access to many of your accounts.

Tips for using Public Wi-Fi Networks

- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- Consider changing the settings on your mobile device so it doesn’t automatically connect to nearby Wi-Fi. That way, you have more control over when and how your device uses public Wi-Fi.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks.

IdentityTheft.gov online reporting



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Report identity theft and get a recovery plan

IdentityTheft.gov can help you report and recover from identity theft.

HERE'S HOW IT WORKS:

Identity Theft Resources

- Federal Trade Commission

  ftc.gov/idtheft

  IdentityTheft.gov

  1-877-ID-THEFT (428-4338

- Federal Bureau of Investigations – FBI

  IC3.gov

- Minnesota Commerce Department

  mn.gov/commerce/consumers/your-money/identity

If you lose money to a scam, call 9-1-1

Request an annual credit report

Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies.

Order online: annualcreditreport.com

Call 1-877-322-8228

- Equifax 1-800-525-6285
- Experian 1-888-397-3742
- TransUnion 1-800-680-7289

STOP. THINK. CONNECT.

is about taking a moment to stop and think about the places we visit online, the information that we share and the communities in which we participate before and while we are connected to the Internet.

Ramsey County Sheriff’s Office

Jack Serier, Sheriff

Questions, Comments and Concerns