SECURING YOUR KIDS

Our Challenge as Parents

- Just like driving, the Internet is a powerful tool our children need to learn how to use.
- Just like driving, it is our responsibility to teach them how to do it safely.
- Unlike driving, our kids know more about the Internet then we do.

The Access Challenge

Our kids have moved way beyond just computers and access the Internet in multiple ways.

- Mobile devices (smartphones, tablets)
- Gaming consoles (Xbox Live, Wii, Nintendo DS)
- Family, friends, school, library

Top Three Risks

- Strangers / Criminals
- Friends
- Themselves

Strangers / Criminals

- Same threats we faced as kids growing up, but online criminals can target more people, and anonymously.
  - Extortion, fraud, identity
  - Predators

- Law enforcement is actively targeting this threat. You can also turn to them if you are concerned about a predator.

Friends

- Same threats we faced as kids growing up, but on a bigger scale and can happen anonymously.
  - Cyber bullying
  - Ex boyfriend / girlfriend.

- Usually law enforcement cannot help you here.

Themselves

- Posting or sharing personal information or pictures. Universities and hiring companies now do background checks on Facebook.

- What kids may think is harmless could be a crime, such as sharing copyrighted materials or hacking sites.

What You Can Do

Education

- Just like the real world, educate your kids on how there are bad people.
- Ensure your kids feel comfortable talking to you. Ask them to explain to you about the technologies they are using.
- Education is your strongest weapon, technology CANNOT keep up. In addition, as kids get older, you have less control.

Dedicated Computer

- Have a computer dedicated just for the kids.
  - Keep it updated / patched with AV and firewall.
  - Make sure each child has their own, non-privelleged account.

- Have your children be responsible for keeping the computer up to date and secure (let them rebuild it when it gets slow).

Mobile Devices

- Have a central, family charging station.
- All devices go there when devices are not in use and before kids go to bed.
- When kids are not at home and have a smartphone, it has to be on, tracking enabled, and they have to respond to all calls from Mom or Dad (no phone dying due too gaming).

Keep It Public

- Keep computer in a public area.
- Keep printer in public area (kids like to print LOTS of colored pages).
- Post family electronics rules (think family Acceptable Use Policy) next to computer.

Online Rules

1. Post by the computer.
2. Have kids review and agree to document, perhaps even have them help develop it.
3. Like any AUP, you will need to update it as kids get older.
   - Times kids can or cannot be online.
   - What they can and cannot do.
   - Who to report any questions or concerns to.

Grandparents

- Just like you train your kids, you may need to train the grandparents.
- When kids are at Grandma’s, what rules apply, are those systems secure?

What happens at Grandma’s stays at Grandma’s

Technology Controls

- Filtering allows you to control what activity your children can and cannot do.

- Monitoring is passive, it only logs and reports what your children were doing.

Filtering

- Most effective for younger children, prevents them from accidently accessing harmful content.
- As children get older, easier to bypass.
- Certain websites are their own ‘ecosystem’ and hard to filter, such as YouTube, Facebook or Instagram.

Monitoring

- Just like at work, allows you to capture online activity.
- When in doubt, log it. You can always disable later.
- For mobile devices, if you want to monitor your kids you have to go with Android.

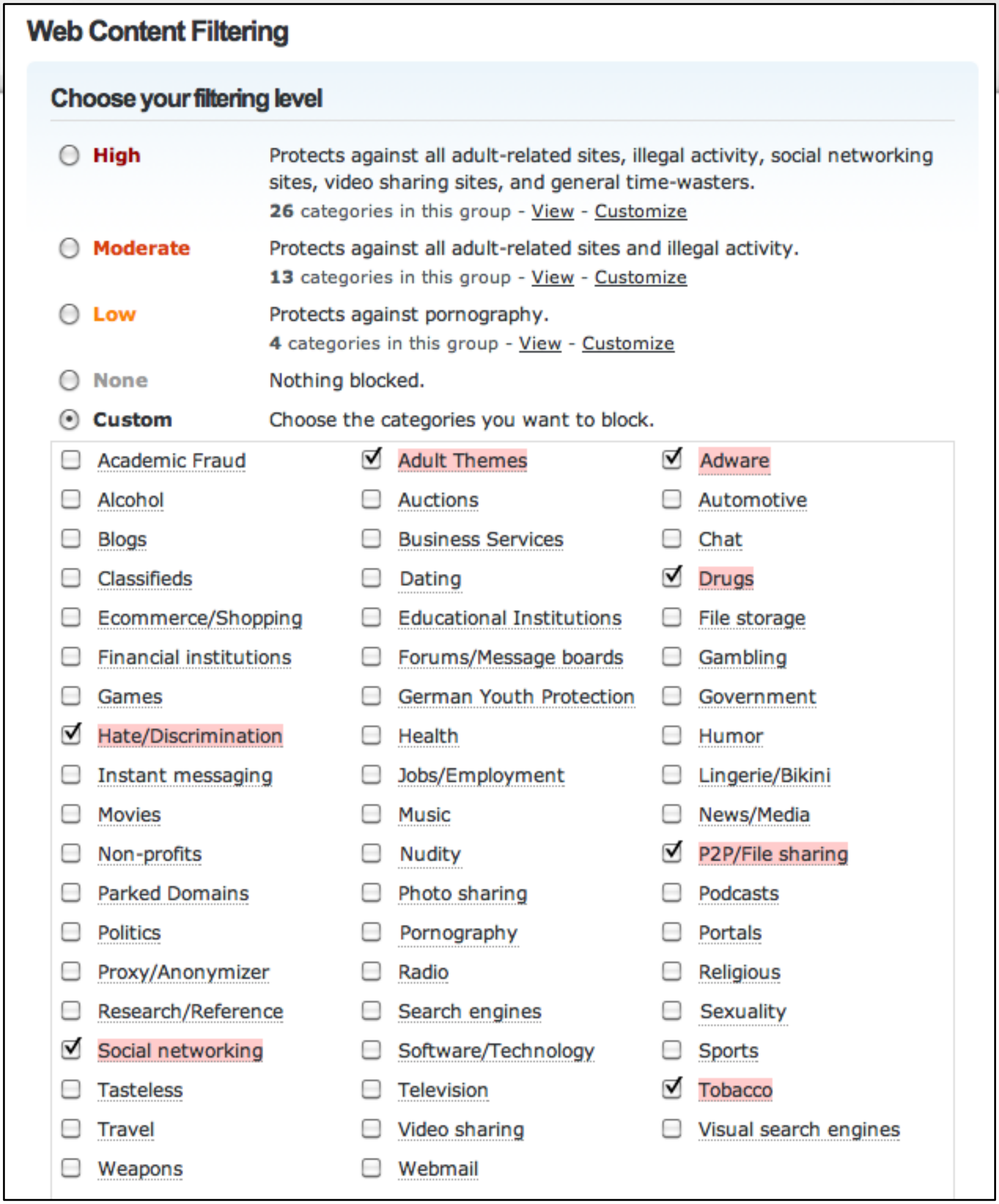
What To Look For

- Can it support multiple devices on multiple operating systems?
- Can it support multiple accounts (one for each child).
- Can you access configuration and reporting remotely or be sent automated reports?

OpenDNS

- Free service.
- Set-up as your DNS server.
- Will block attempts to connect to any server based on settings.
- Excellent for filtering website activity and protecting against malicious sites.
- Poor reporting.

http://www.opendns.com



Web Content Filtering

Choose your filtering level

○ **High** — Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.
26 categories in this group - View - Customize

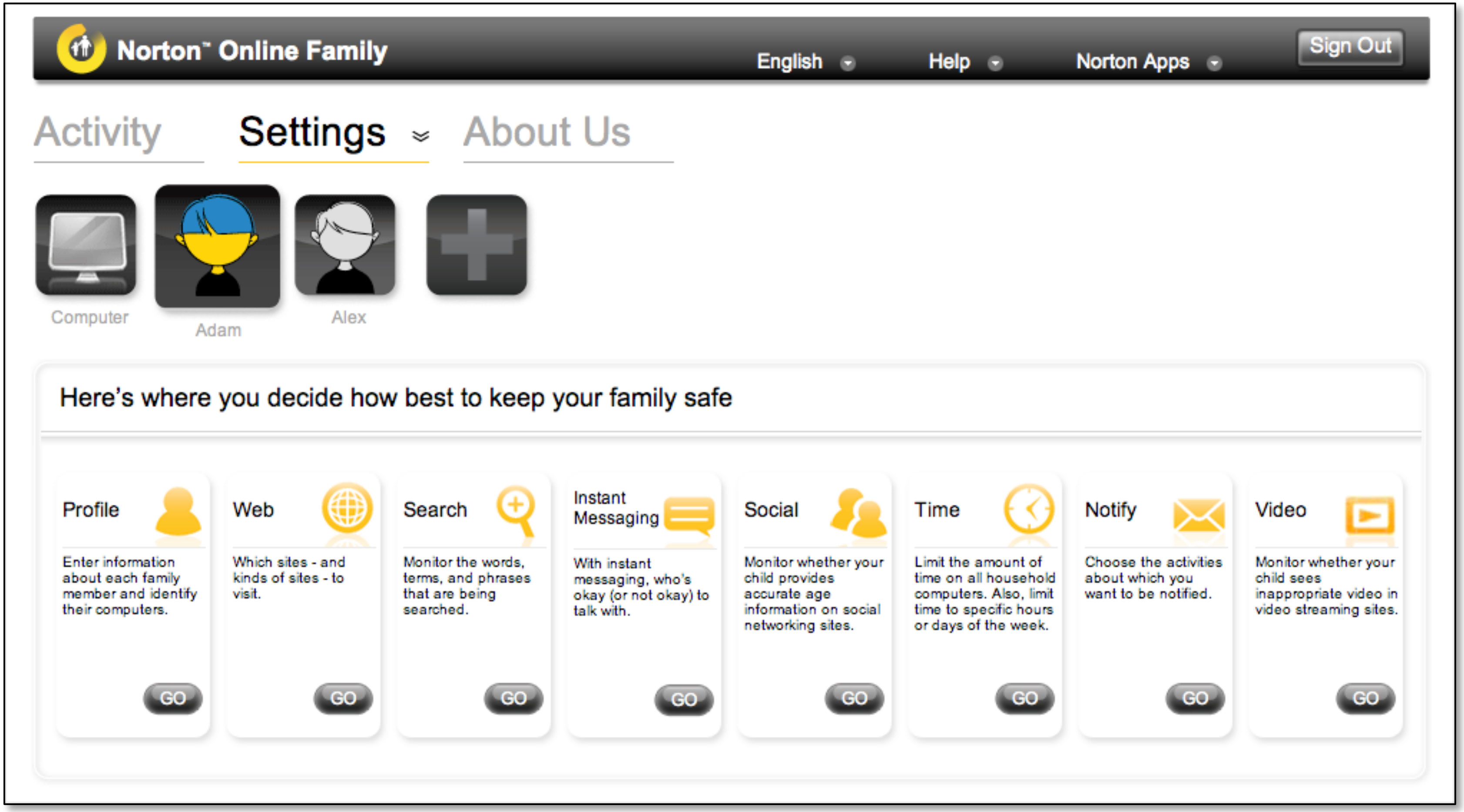
○ **Moderate** — Protects against all adult-related sites and illegal activity.
13 categories in this group - View - Customize

○ **Low** — Protects against pornography.
4 categories in this group - View - Customize

○ **None** — Nothing blocked.

● **Custom** — Choose the categories you want to block.

□ Academic Fraud	☑ Adult Themes	☑ Adware
□ Alcohol	□ Auctions	□ Automotive
□ Blogs	□ Business Services	□ Chat
□ Classifieds	□ Dating	☑ Drugs
□ Ecommerce/Shopping	□ Educational Institutions	□ File storage
□ Financial institutions	□ Forums/Message boards	□ Gambling
□ Games	□ German Youth Protection	□ Government
☑ Hate/Discrimination	□ Health	□ Humor
□ Instant messaging	□ Jobs/Employment	□ Lingerie/Bikini
□ Movies	□ Music	□ News/Media
□ Non-profits	□ Nudity	☑ P2P/File sharing
□ Parked Domains	□ Photo sharing	□ Podcasts
□ Politics	□ Pornography	□ Portals
□ Proxy/Anonymizer	□ Radio	□ Religious
□ Research/Reference	□ Search engines	□ Sexuality
☑ Social networking	□ Software/Technology	□ Sports
□ Tasteless	□ Television	☑ Tobacco
□ Travel	□ Video sharing	□ Visual search engines
□ Weapons	□ Webmail	



Here's where you decide how best to keep your family safe

Profile
Enter information about each family member and identify their computers.
GO

Web
Which sites - and kinds of sites - to visit.
GO

Search
Monitor the words, terms, and phrases that are being searched.
GO

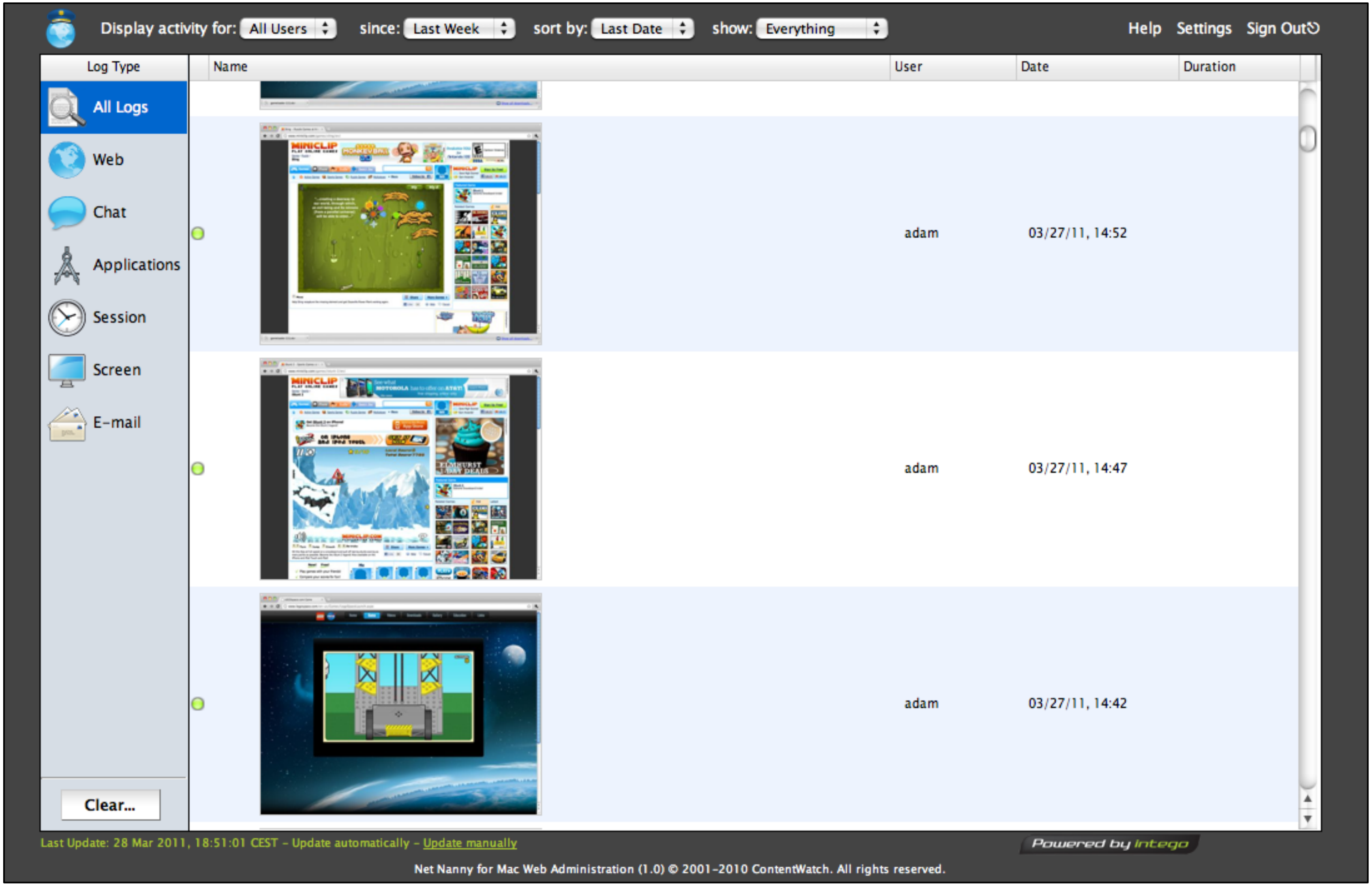
Instant Messaging
With instant messaging, who's okay (or not okay) to talk with.
GO

Social
Monitor whether your child provides accurate age information on social networking sites.
GO

Time
Limit the amount of time on all household computers. Also, limit time to specific hours or days of the week.
GO

Notify
Choose the activities about which you want to be notified.
GO

Video
Monitor whether your child sees inappropriate video in video streaming sites.
GO



Display activity for: All Users since: Last Week sort by: Last Date show: Everything

Name	User	Date	Duration
	adam	03/27/11, 14:52	
	adam	03/27/11, 14:47	
	adam	03/27/11, 14:42	

Last Update: 28 Mar 2011, 18:51:01 CEST – Update automatically – Update manually

Powered by intego

Net Nanny for Mac Web Administration (1.0) © 2001-2010 ContentWatch. All rights reserved.

Other Options

- Windows – Family Safety 2011
  - http://windows.microsoft.com/en-us/windows/set-up-family-safety#
- Mac OS X
  - System Preferences – Parental Controls
- Monitor phone bills. Most service providers now have parental contorls.
- Create a FB/Instagram account and *friend* your kids.

Cyber Aces

- Have a teenager that loves technology and attracted to hacking? Great! Channel that passion into good.
- Cyber Aces: Free online cyber security training and testing.
- Gain access to international competitions.
- Gain access to National Cybersecurity Career Fair.

www.cyberaces.org

Set a Good Example

- Explain to kids how to setup a secure system, then have them help you maintain it.
- Sit down with them and teach them what to look for and when to tell you.
- When in doubt, have them show you what apps they are using and how they work.

Top Take-Aways

1. Education is key, continually talk to them what is appropriate, what is not appropriate and what dangers to look out for.
2. Have a dedicated computer / charging station for your kids and keep in in open area.
3. Post agreed upon rules.
4. Filter / monitor their activities as you see fit when they are younger, but realize these will be less effective as kids get older.

Resources

- http://ikeepsafe.org/
- http://www.microsoft.com/protect
- http://www.facebook.com/safety
- http://www.onguardonline.gov
- http://www.securingthehuman.org/ouch

Creating a Cyber Secure Home

1 You

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.

To learn more, visit
www.securingthehuman.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 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