

# OUCH!

## IN THIS ISSUE...

- Overview
- The Basics
- Visiting Kids

## Securing the Cyber Generation Gap

### Overview

Many of us feel comfortable with technology, to include how to use it safely and securely. However, other family members may not feel so comfortable with technology, especially if they did not grow up with computers or the Internet. Here are some steps you can take to help secure the generation gap. In addition, you may be taking steps to secure your children at home, but similar security measures may not exist when your kids visit a relative's house. As such, we will also cover how you can help create more secure online environments when your kids visit these relatives.

### Guest Editor

Brian Honan (Twitter [@brianhonan](https://twitter.com/brianhonan)) is an independent security consultant based in Dublin, Ireland. He is founder and head of Ireland's first CERT, a Special Advisor to Europol's Cybercrime Centre (EC3) and lectures on Information Security at University College Dublin. He has authored a number of books and writes for various industry publications.

### The Basics

Just a few basic steps can go a long way to securing anyone's digital life. Here are the basic steps we always recommend for any family member. However, if you know a family member who does not understand these steps, you may have to walk them through these steps or implement them yourself.

- **Social Engineering:** Explain the concept of social engineering in simple terms that anyone can understand. Scams and con artists have existed for thousands of years; these types of attacks are not new. The only difference now is that bad guys are applying these same concepts to the Internet. Give examples of the most common scam attacks today, such as common phishing emails or the infamous Microsoft tech support phone calls. If nothing else, make sure family members understand they should never give their password to anyone or allow remote access to their computer. Finally, be sure they know that if they feel uncomfortable or have questions about an email or someone calling them, that they call you first before giving up any information.
- **Home Wi-Fi Network:** Take time to make sure the Wi-Fi network at their home is secured. At a minimum, make sure the default admin password has been changed, there is a strong password to access the home

## Securing the Cyber Generation Gap

Wi-Fi network and the network connection is using the latest encryption. You may also want to consider configuring the Wi-Fi network to use a secure form of DNS, such as [www.opendns.org](http://www.opendns.org). Secure DNS services not only help stop people from visiting infected websites, but can give you control over the websites people can or cannot visit, which may be valuable for visiting kids.

- **Patching:** Keeping systems current and fully up-to-date is one of the most fundamental steps you can take to securing any technology. As such, make sure all home devices (including mobile devices) and applications are fully patched. The simplest way to ensure this is to enable automatic updating wherever possible.
- **Anti-Virus:** People make mistakes. We sometimes click on or install things we probably should not have. While anti-virus cannot stop all malware, it does help detect and stop the more common attacks. As such, make sure any home computer has anti-virus installed, and that it is current and active.
- **Passwords:** Strong passwords are key to protecting both devices and any online accounts. Walk your family members through how to create strong passwords. Passphrases may be easiest for them to both use and remember. Another idea is to install a password manager and teach them how to use it. If that does not work, perhaps teach them to write their passwords down, and then store those passwords in a secure location that only they can access. You may also want to set up two-step verification for any critical online accounts.
- **Backups:** When all else fails, backups will save the day. Make sure family members have a simple, reliable file backup system in place.

You may want to do a monthly or quarterly check to make sure all these steps are also in place. In a worst-case scenario, consider installing remote administrative software on a device; however, if you do so, make sure it is secured with both encryption and a strong, unique password.



*Older generations may need help securing their home technology and creating a safe environment for any visiting children.*

## Securing the Cyber Generation Gap

### Visiting Kids

Quite often, when young kids visit a relative's house, such as their grandparents, the rules you have at your own house may no longer exist. This can include rules designed to help protect your kids online. Here are some steps you can take to help protect kids:

- **Rules:** Be sure that if there are any rules or expectations you have for your kids' security, relatives know about them. For example, are there any rules on how long kids can game online or when they can have access to their mobile devices? Trust us: don't plan on your kids explaining the rules to their grandparents or other family members. One idea is to create a 'rules sheet' and share that with any relatives your kids frequently visit.
- **Control:** If your children understand technology better than their guardians do, they may take advantage of that. For example, kids may ask for or gain administrative rights to a grandparent's computer and then do whatever they want, such as installing that game you may not want them playing. Make sure that relatives understand that they should not give the kids any additional access beyond what has been established.

### Industrial Control System Security

Be sure to check out our free security awareness resources, including our blog and Video of the Month. This month, we are covering Industrial Control System (ICS) Attacks. View how a real ICS attack could happen at <http://www.securingthehuman.org/u/2uX>.

### Resources

Social Engineering:	<a href="http://www.securingthehuman.org/ouch/2014#november2014">http://www.securingthehuman.org/ouch/2014#november2014</a>
Securing Your Home Network:	<a href="http://www.securingthehuman.org/ouch/2014#january2014">http://www.securingthehuman.org/ouch/2014#january2014</a>
Passphrases:	<a href="http://www.securingthehuman.org/ouch/2015#april2015">http://www.securingthehuman.org/ouch/2015#april2015</a>
Anti-Virus:	<a href="http://www.securingthehuman.org/ouch/2014#december2014">http://www.securingthehuman.org/ouch/2014#december2014</a>
Protecting Your Kids Online:	<a href="http://www.securingthehuman.org/ouch/2013#april2013">http://www.securingthehuman.org/ouch/2013#april2013</a>
Tech Phone Support Scams:	<a href="http://www.onguardonline.gov/articles/0346-tech-support-scams">http://www.onguardonline.gov/articles/0346-tech-support-scams</a>
Creating a Cyber Secure Home Poster:	<a href="http://www.securingthehuman.org/resources/posters">http://www.securingthehuman.org/resources/posters</a>

### License

OUCH! is published by SANS Securing The Human and is distributed under the [Creative Commons BY-NC-ND 4.0 license](http://creativecommons.org/licenses/by-nc-nd/4.0/).

You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit [www.securingthehuman.org/ouch](http://www.securingthehuman.org/ouch). Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](http://securingthehuman.org/gplus)