

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- Top Three Threats
- Protecting Your Children
- Resources

Protecting Your Kids Online

GUEST EDITOR

Kevin Johnson is the guest editor for this issue of OUCH! Kevin is the CEO at Secure Ideas, runs MySecurityScanner.com and is a senior instructor with the SANS Institute. You can find out more information at www.secureideas.com.

BACKGROUND

We all want the best for our children, including the ability to leverage technology. However, with technology come risks, risks that our children are often not aware of or prepared to deal with. As parents, it is our responsibility to ensure our children understand these risks and how to protect themselves. But this can be challenging, as we ourselves did not grow up in the same environment. In this newsletter, we explain the top three online threats to your children and how you can help them stay safe.

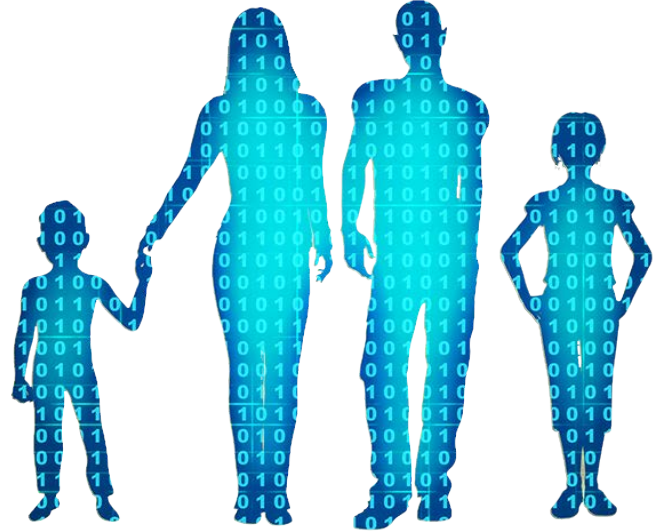
TOP THREE THREATS

To protect your children, you have to first understand the dangers they face online.

1. **Strangers:** This is one of the most common threats parents think of when wanting to protect their kids online. In this context, strangers are individuals (usually adults) who establish online relationships with your children in order to take advantage of them, such as sexual predators. Often, these individuals pretend to be children themselves.
2. **Friends:** These are people your children already know, and are often other kids at school. Friends can pose a serious threat as online bullies. Remember that bullying no longer means just physical confrontation. In fact, the Internet amplifies the issue, as bullies can post harassing messages to the entire world or hijack your child's identity online. In addition, bullies can launch these attacks anonymously, making them harder to track down and stop. Finally, anonymity makes it easier for someone to become a bully, since there is less chance of retribution.
3. **Themselves:** In today's world of social networking children can be their own worst enemy. Anything they post is accessible not only to the entire world, but once

Protecting Your Kids Online

posted may also be difficult or even impossible to remove. Your children may not realize how these postings can impact their future. It is becoming a standard practice for universities and employers to review peoples' social networking activities and Internet presence. Anything embarrassing or illegal posted by or about your children can negatively impact their future. In addition, highly personal information can be used by strangers-- or even by friends --to target or harm them or your family.



PROTECTING YOUR CHILDREN

Now that you understand the key risks, here are steps you can take to defend against them:

- **Education:** The most important step you can take is education. Make sure your children understand these threats and that you are always talking to them about their online activities, staying current with what they are doing. In addition, create an environment where your children feel comfortable coming to you with questions or problems they may have online.
- **Dedicated Computer:** Have a separate computer just for your children. This helps ensure that if they do accidentally infect their computer, your own accounts, such as online banking, are not affected or compromised. In addition, keep the children's computer in an open area in your home so that you can monitor their online activities. Finally, make sure each child has and uses their own, non-administrative account on their computer. This will make it possible

The key to protecting your children online is to educate them about the risks they face and set expectations for what is and is not allowed.

for you to track and enforce what each child is doing on the computer.

- **Mobile Devices:** Mobile devices can be more challenging. For mobile devices, consider setting time limits when your kids can use them; at all other times they have to turn in their devices to you (perhaps create a central family re-charging station). Also consider taking your kids' mobile devices at night so they are not tempted go online when they should be sleeping.
- **Social Networking:** Track what your children are doing online by creating your own accounts on social networking sites such as Facebook, Twitter or

Protecting Your Kids Online

Instagram and then have your children invite you so you can follow what they publish.

- **Rules:** Create a document that identifies the rules you expect your children to follow when online. Rules can include when they can use technology, for how long, what games or apps they can and cannot play and what information they can or cannot post online. Also, consider posting how the rules will be enforced, and possible consequences for violating the rules. Review the document with your kids and then post it by their computer so that your children will know and understand your expectations.
- **Technology:** Finally, there are technologies you can use that help filter and monitor your children's online activities. Most operating systems come with parental controls, and there are additional free and commercial tools you can use, such as OpenDNS. Security technologies are useful for younger children; however, as children grow older, technology becomes less effective. Not only do older children need greater Internet access for school or work, but they will also be using devices you do not control at libraries, at a friend's or relative's house, or at school. In addition, some mobile devices lack strong parental control software, such as iPads or iPhones. This is why education and the rules you create are far more effective than depending on technology alone.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

11 Security Tips for Online Social Networking:

<http://preview.tinyurl.com/b28a525>

FB Security:

<https://www.facebook.com/safety>

Your FB Security Settings:

<https://www.facebook.com/settings?tab=security>

Common Security Terms:

<http://preview.tinyurl.com/6wkpa5>

SANS Security Tip of the Day:

<http://preview.tinyurl.com/6s2wrkp>

BECOME A SECURITY PROFESSIONAL

Become a certified security professional from the largest and most trusted security training organization in the world at SANSFIRE. Over 40 security classes taught by the world's leading experts. 14-23 June in Washington DC. <http://www.sans.org/event/sansfire-2013>

OUCH! is published by the SANS Securing The Human program and is distributed under the [Creative Commons BY-NC-ND 3.0 license](https://creativecommons.org/licenses/by-nc-nd/3.0/). Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner