# Internet Safety

First Alert
PROFESSIONAL SECURITY SYSTEMS®

# Internet safety

Everywhere you look these days, more and more people are surfing the Internet. According to Internet World Stats, by the end of 2007, there were over 237 million people using the Internet in North America alone!

With its increased popularity, the threat of Internet crime is a serious concern. Unfortunately, criminals have caught up with technology and a variety of Internet crimes are occurring regularly against adults and children.

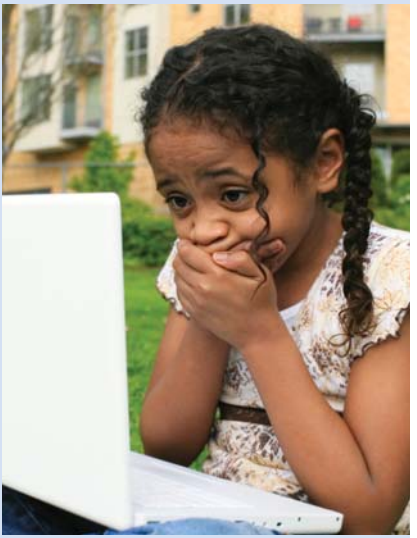
Honeywell and First Alert Professional Security Systems are committed to public safety. We manufacture electronic security and fire detection systems that are protecting homes and businesses worldwide. That is why we have developed this booklet to help educate families about security on the Internet. We hope it will help you and your family to be aware of the dangers lurking in cyberspace. The Internet can be a fun tool; but please remember to use it with caution.

# Contents



# Children and the Internet

**The Internet can be a fun and educational resource for children. Where else can you research school projects, play games and chat with friends? But if it isn't used properly, the Internet can also be very dangerous.**



## Let's Review Some Simple Safety Rules That Families Should Follow:

### 1. Keep the Computer in a Family Room

When you place the computer in a family room, instead of a child's bedroom, the computer screen can be seen by everyone. This way it is much easier to keep an eye on Internet usage.

### 2. Install Parental Controls

Before you let your children use the computer, it's a great idea to install parental controls. These can be found through your Internet Service Provider or you can purchase special blocking software. Although these filters are a great first step, they can't block out every danger. Make sure you consistently monitor your family's usage of the Internet.

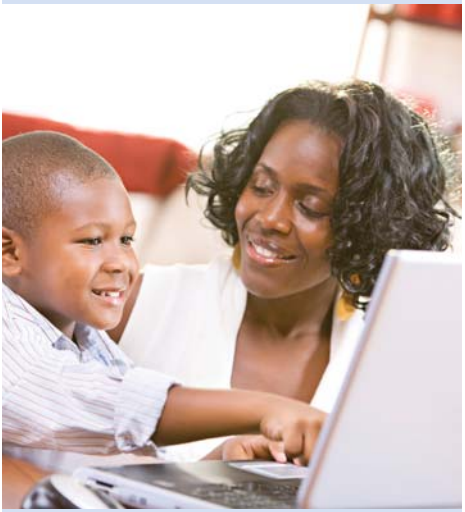
### 3. Learn What Your Child is Doing

It's important to get to know how your child is using the Internet. One way to learn is through first-hand experience. Sit with your child and have him/her show you what he/she does online. Who knows, you might learn a thing or two about the Internet in the process!

# Important guidelines to tell your children about Internet usage

## 1. Never Chat with People They Don't Know

On the Internet, it is very easy for child predators to pretend to be someone else behind a computer screen. A 55 year-old-man can say he is a 14-year-old-girl and your child wouldn't know the difference. These predators can lure children into meeting or speaking with them offline, so it's extremely important for you to make your child aware that they should never chat on the Internet with people they don't know.



## 2. Never Give Out Personal Information

When children are online, they should never offer personal information. Explain to your children that this includes their name, where they live, their computer password, even the name of their school or sports team. Digital photos should never be shared. Your children may not think anything of sharing this information, but predators can use this information to gain their trust.

## 3. If They Feel Uncomfortable, Tell a Trusted Adult

Since there are so many unsafe things that can happen, it's impossible to predict every scenario. Instruct your children to tell you whenever they are uneasy about things they are doing. If your children tell you about something that makes them uncomfortable, you can report what happened to the CyberTipline by calling 1-800-843-5678. This safety organization will ask questions about the event, and give you information about people who can help.

# Chat rooms

**Chat rooms** can be a fun experience. You can share views on politics, TV shows, etc. However, you should exercise caution when participating in chats. Be sure to log into a chat room using an alias, or nickname, as opposed to your user name. Also, do not give out personal information about yourself, such as where you live, where you work, etc. Incidents of online stalking and harassment are on the rise. Online, it is easier to become someone else since there is no face-to-face interaction. Remember that people you are speaking with may not be who they say they are.

**Online stalkers** commonly use the Instant Message feature to contact their victims. (This is a program that allows you to speak to someone in "real time," with only the sender and receiver possessing the ability to see the active window.) These predators enter chat rooms and look up profiles of the participants until they find a profile that appeals to them. Once they decide on the person they want to contact, an Instant Message is sent to the person. If you receive an Instant Message from someone you do not know, do not respond. Remember that you cannot be certain who is on the other end of this message, and they should be treated the same as a stranger who contacts you by phone or out in public.

**Always exercise caution while surfing the Internet.** As mentioned, do not give out personal information in chat rooms or via instant messages from someone you don't know. Check into your Internet Service Provider's privacy policy as well. Many online services have a "user profile." Do not fill out any personal information other than your first name. By submitting personal information to the millions of Internet users out there, you are increasing your chances of a stranger learning more about you than they should, thus increasing your chances of being victimized.

### Steps to follow if you believe your child has been victimized online

- If you know about a child who is in immediate risk or danger, contact your local law enforcement agency.
- To report incidents of child sexual exploitation, contact the National Center for Missing & Exploited Children's (NCMEC) 24-hour CyberTipline at www.cybertipline.com, or call 1-800-843-5678.
- For more information about how to better protect your children online, contact the NCMEC at www.missingkids.com, or call 1-800-THE-LOST (1-800-843-5678).

# E-mail safety

## To keep your computer safe, follow these e-mail safety rules.

### 1. Get Rich Schemes/Sweepstakes Offers

You receive an e-mail where the subject says you won a prize or alerts you of a way to make money, fast. If it sounds too good to be true, it usually is. Delete the e-mail without even opening it.

### 2. Computer Viruses:

- To avoid a computer virus from infecting your computer, always check the address of the person who e-mailed you. Only open e-mails from addresses you recognize.
- If you receive an unsolicited commercial message, don't open it if the attached file has an address ending in ".exe."
- **Invest in Virus Protection:** Install a current anti-virus program, in the event that someone you know inadvertently infects your computer. It's important to keep these programs up to date since new viruses are created frequently.
- **Blocking Programs:** Check with your Internet Service Provider about their rules regarding unwanted e-mails. Many times they have a solution to block unwanted e-mails from reaching your mailbox.

### 3. Beware of Phishing

Phishing is a term used to describe when computer hackers use e-mail to fish the Internet hoping to hook you into giving them your login, passwords and/or credit card information. How do these scams operate? The phisher first pretends to be a legitimate company such as your Internet Service Provider or bank. In the scam, you get an e-mail that appears to be from a reputable company. You're then asked to go to a special site to update your account information. If you get one of these e-mails, don't open it and report it to your Internet Service Provider immediately.

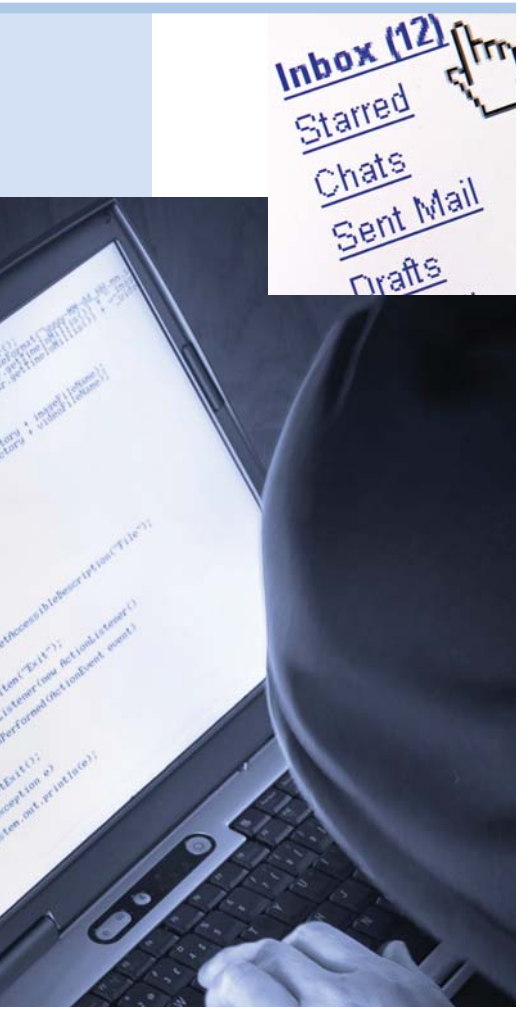
### 4. Think You've Been Phished?

**If you think your information has been phished, take immediate measures to minimize the damage.**

- If you were lured by an imposter of a legitimate company, get in touch with the actual company immediately.
- If you provided credit card information, contact your credit card company and speak to someone in risk management or loss prevention.

# Spam E-mail

E-mail is an affordable way to stay in touch and a vital tool in the workplace. Now that companies have realized the marketing potential of the Internet, your computer is probably being inundated with e-mails from unwanted sources. Better known as spam, these e-mails can be annoying and time consuming. According to Anti Spam, it is estimated that just under 100 billion spam messages are sent worldwide every twenty-four hours.



# e-Commerce

According to a report from Forrester Research, U.S. online retail sales will reach $335 billion by 2012. Emarketer reports that by 2011, Canadian online spending will more than double, reaching C$37.2 billion. If you are going to use this convenient method of shopping, you need to protect yourself from the threat of fraud and theft.

# Online shopping safety tips

## 1. Make Sure Your Browser is Secure

On most browser toolbars, you will find a “Tools” section. Click on this section and find the “Security” Tab. Enter in the level of security you want the browser to contain. Install security updates as they are made available.

## 2. Use Secure Internet Connections:

- Many sites use Secure Sockets Layer (SSL) technology to encrypt credit card information. Check if the Web address where you input your credit card information begins with “https:” instead of “http:”. If it does, then SSL technology is in place.

- Your browser can also display the icon of a locked padlock or unbroken key at the bottom of the screen, or a lock on the status bar. All of these icons indicate that the site is secure.

## 3. Use Different Passwords

If you have a password to log onto your computer, use a different one for shopping orders.


## 4. Don’t Write Down Passwords Near Your Computer

This may sound like common sense, but often people write down their password, only to have it be used against them. If you need to keep your password close to the computer, reverse the order of the characters to keep your true password secure.

# The Internet has opened up many possibilities

**Along with these possibilities come numerous safety concerns. We hope you find this booklet useful in helping to protect your family against Internet crime. By practicing some of the safety tips mentioned, you may reduce your risk of becoming victimized by the dangers that lurk in cyberspace.**

Developed with assistance from the:
**National Crime Prevention Council**
**www.ncpc.org**

**National Center for Missing & Exploited Children**
**www.ncmec.org**

Developed with information from the:
**Better Business Bureau**
**www.bbb.org**

Honeywell is a proud partner of the:
**National Crime Prevention Council,** and the
**National Center for Missing & Exploited Children.**

Whether you live in a city, suburb or rural community, the presence of crime has become an inescapable reality. It threatens us, our children and our property. One of the best ways to help keep your family safe and protect your property is by selecting a professionally installed security system from First Alert Professional.

Why you should choose a First Alert Professional authorized dealer:

Our selected dealers are among the best in your community. They operate reliable businesses you can count on. Their commitment to your community is evident in the quality of their service and their outstanding reputations.

Most importantly, First Alert Professional authorized dealers are dedicated to the safety of their customers in the communities they serve. We, at First Alert Professional, have a strong commitment to life safety and community service. Our award winning training programs, thorough life safety program and innovative community service initiatives provide our dealers with a great competitive advantage.

The information provided in this pamphlet provides general information obtained from sources that have not been verified for completeness or accuracy. We make no representations as to the accuracy of this information and will not be liable for any damages resulting from reliance on this information. The information provided is for educational purposes. The information is not a substitute for the advice of professionals.

www.firstalertprofessional.com

Honeywell

First Alert
PROFESSIONAL SECURITY SYSTEMS®

April 2008 FA/INTSAFEB 