

# ONLINE SAFETY FOR SENIORS



# The Internet

---

The Internet is a fantastic place to learn, communicate, meet people, shop, bank, conduct business, plan travel, access records, stay in touch with friends and family, and do so much more.

With a few precautions you can get the most from the Internet -- safely!

# Internet Safety Issues

---

- Lack of knowledge about online safety risks
- Carelessness in online activity
- Exposure (unintentionally or intentionally) of personal information by others
- Security flaws and/or breaches in products or software

# Internet Safety Risks

---

- Often we think about online risks in the context of kids – sexual predators, inappropriate material, and bullying, BUT
  - The risks are the same *regardless* of your age
- In reality, the biggest dangers online come from our own lack of understanding of the risks (and how to avoid them). Here are 3 big ones:
  1. Failure to consider what information we share and making poor decisions about whether information should be shared
  2. Failure to identify trustworthiness – of people, Web sites, content, and businesses we deal with online
  3. Failure to understand how predatory behavior works and to spot it before you become a victim

# Use Technology to Stay Safer

---

The #1 safety action you can take: secure your computer and home network

## Protect your computer

- Install antivirus, firewall and anti-spyware software and set these to update automatically. There is good, free software available.
- Use a reputable browser such as Internet Explorer, Firefox or Safari, and keep the default security and privacy settings intact
- Check for and install software updates for your Operating System and browser. Use the automatic update feature for Microsoft OS

## Protect your home network

- If you use a wireless home network, make sure it is secured
- Make sure your firewall software is enabled

# Use Technology to Stay Safer

---

The #2 Safety action: secure your browser

## Identify Safe Websites

- If you get a notification from your antivirus/antispymware program, that a site you are trying to visit is unsafe, believe it. Don't go there.
- If a site asks you to change your browser settings in order to "improve your experience" ignore the request and go to a different website.
- Only allow downloads of programs that come from websites you visit (not sites you may be re-directed to by another site), and only do so when you absolutely trust and understand what the program will do.

# Be Smart -- Use Email Safely

---

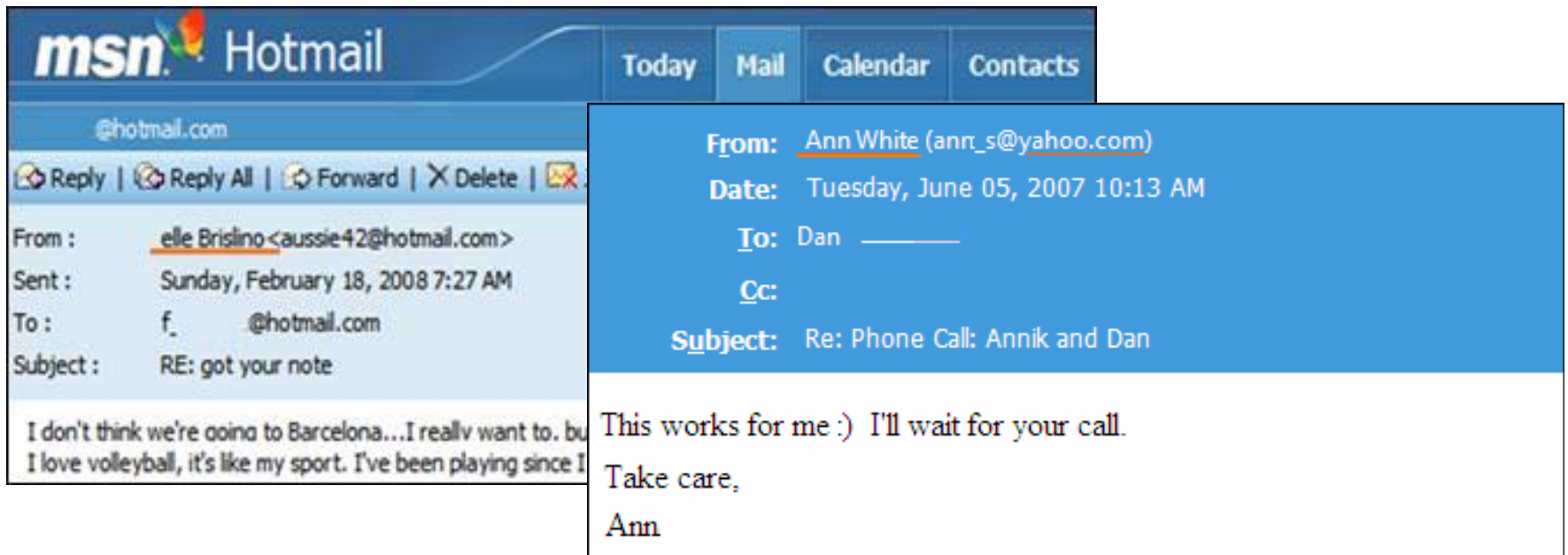
A few key skills go a long way:

- Create “safe” aliases and nicknames
- Use “strong” passwords
- Never send a password or sensitive account information via email
- Never click on a link embedded in an email you receive
- Never click on a link in an email asking you to visit a website to “update” your User ID or Password
  - No legitimate business will ever ask you for your User ID or Password

These will help you avoid Spam, Scams, & Phishing, viruses and other malicious code

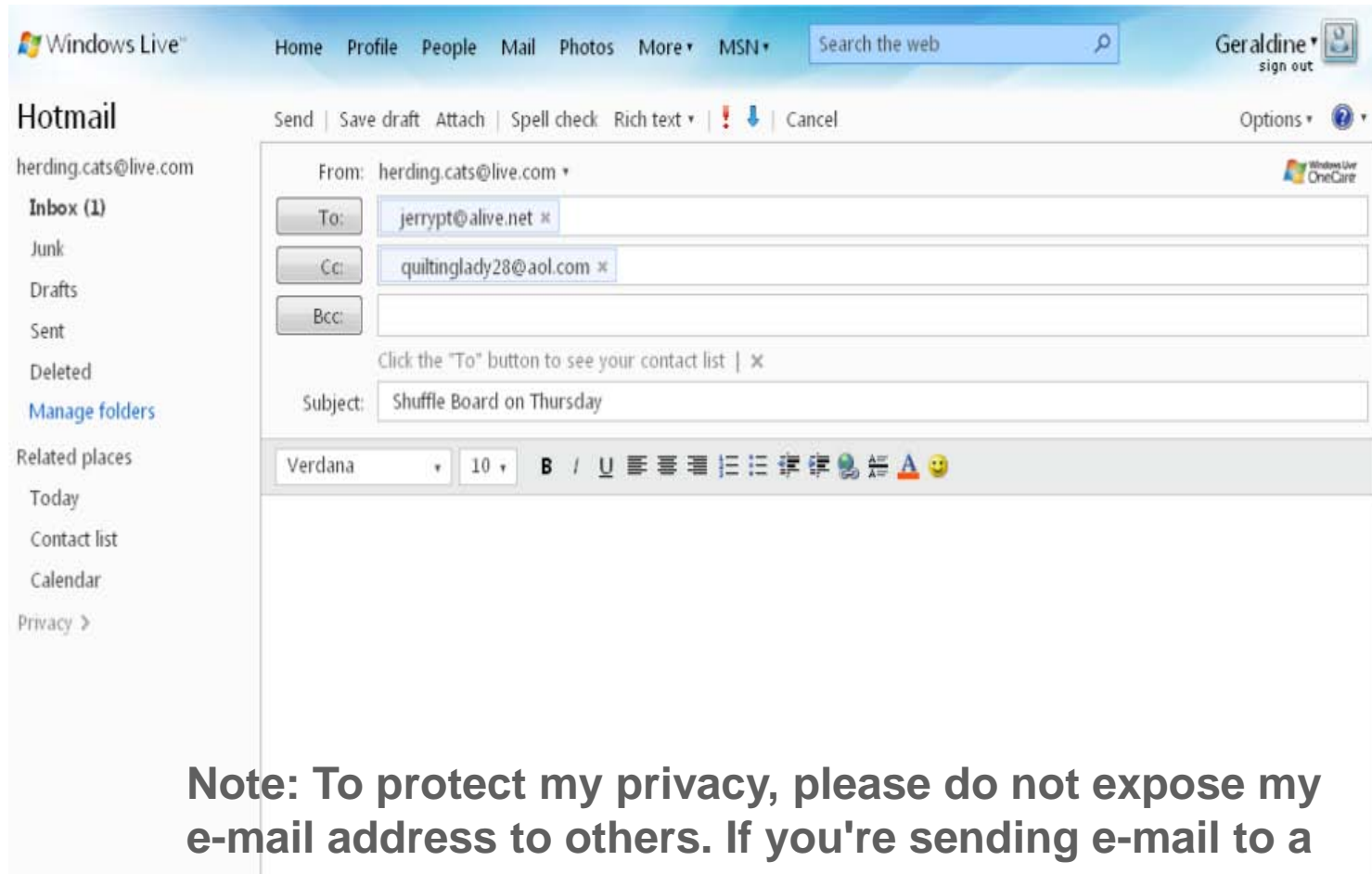
# Use Safe Email Addresses

- Don't use an email address with your name, age, location, or interest affiliation
  - TracyJordan1952@email.com
  - CathyBurns\_Seattle@email.com
  - Soccer\_Fan@email.com



The screenshot shows a Hotmail email interface. The top navigation bar includes 'msn Hotmail', 'Today', 'Mail', 'Calendar', and 'Contacts'. The email header shows the sender as 'elle Brisino <aussie42@hotmail.com>' and the recipient as 'f. @hotmail.com'. The subject is 'RE: got your note'. The email body contains the text: 'I don't think we're going to Barcelona... I really want to. bu I love volleyball, it's like my sport. I've been playing since I'. A blue pop-up window displays the email details: 'From: Ann White (ann\_s@yahoo.com)', 'Date: Tuesday, June 05, 2007 10:13 AM', 'To: Dan', 'Cc:', and 'Subject: Re: Phone Call: Annik and Dan'. Below the pop-up, the text 'This works for me :) I'll wait for your call. Take care, Ann' is visible.

# Forwarding Email Respectfully



**Note: To protect my privacy, please do not expose my e-mail address to others. If you're sending e-mail to a group of people that includes me, please put my e-mail address on the Bcc: line only.**

# Use Strong Passwords

---

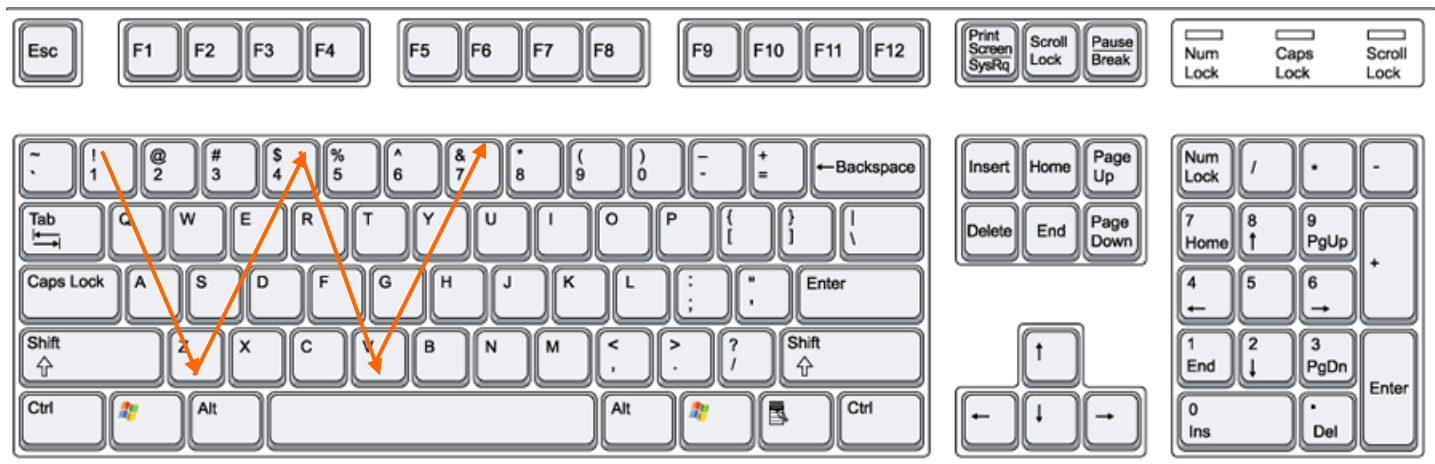
## Safe passwords must:

- Be Long: Use at least 10 characters
- Be Strong: Include capitals, characters, and numbers
- Be Obscure: Include nothing that's associated with you, your family, your company, and so on
- Protect Your Passwords: Keep them secret. Don't place paper reminders near your computer. And don't use the same password for sensitive and non-sensitive websites
- Change Your Password: The more sensitive the information, the more often you should change your password



# Use Strong Passwords

- Safe passwords don't have to be hard to remember, just hard to guess.
  - 2BorNot2B?
  - Looking@myBank
  - MayB\_L8r
  - 1qazse4rfvgy7



# Spotting Spam and Scams

---

Most email spam and scams are easy to spot:

- You don't know the person sending the e-mail
  - The claims sound too good to be true
  - They promise to send you money or a prize
  - A financial institution or store asks for your account information or password
  - You're asked to click on a link in the e-mail or download a file
  - The message has misspellings or is otherwise unprofessional
  - Someone wants to give you money
- 
- The more dangerous scams are the ones that you think *might* be legitimate – an email that looks like it's from a company you have an account with or that contains text warning you against fraud
  - Stay safe by always logging into your account yourself. If you don't know the real URL by heart, use a search engine to find it and then bookmark the link. Never click on a link in the email



# Identity Theft


---

- More than 200 million records containing personal information have been reported stolen or lost in the U.S. since 2004
  - We don't know how many were not reported
- ID theft steals more than your money
  - It steals your sense of safety
  - Time in cleaning up your credit history
  - Requires extra diligence forever
  - May place other family members at increased risk of having their identities stolen.
- Key takeaway: Be careful about the information you share about yourself and your family



# Information Shared on Blogs

Log in or Sign up Home People Fun Love Money Body LifeDreams Obits LifeMap Travel My profile Invite Size: A A

 50 plus everything...

**Road Scholar®** *click here*  
Register to win a free trip for two to Alaska with Road Scholar — and sail the coasts of the Denali Peninsula under the midnight sun.

**Christina Ryan** | Sebastian, FL





Search members  Go [Browse members](#)

**About me** 3  
I have had varied career leanings including the insurance industry and the beauty world. Currently I am the office administrator for a cosmetology school in FL.




**Where Christina Ryan's been** 4  
Hometown: [I grew up in North Reading/Andover, MA](#)  
High School: [North Reading High School](#)  
College: [Andover Business School--MA](#) [Northeastern University--MA](#) [Melrose Beauty Academy--MA](#) [MA Academy of Cosmetology--FL](#)

**Christina Ryan's** 1  
62, Female  
Marital Status: [Single](#)  
Located in [Sebastian, FL](#)  
[Send a private message](#)  
[Add to my favorites](#)

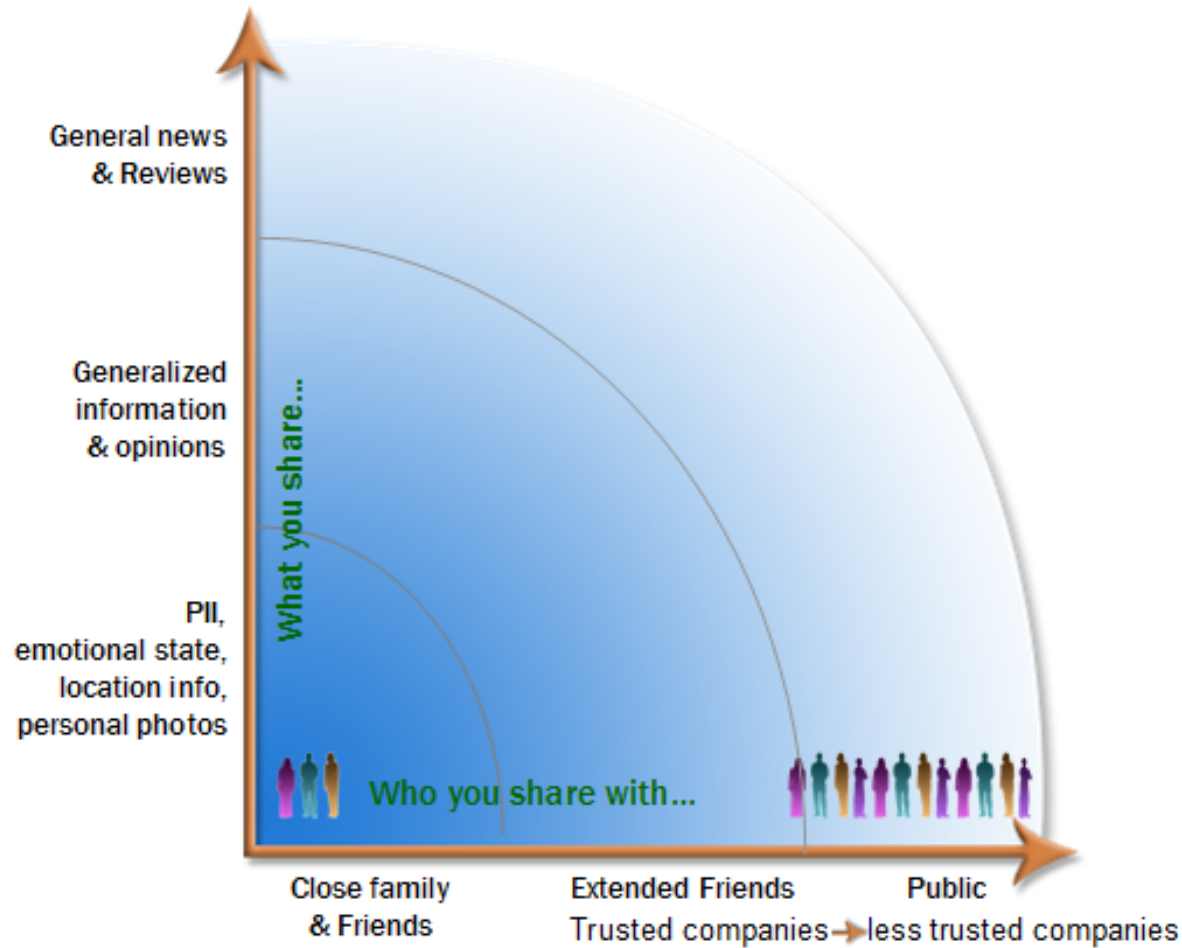
**Christina Ryan's questions of the day** 5  
What are you buying at the farmers market?  
If it's not at the supermarket, I'm not buying it  
Are you saving for retirement?  
No, I can't  
Who is the first person you would tell if you won \$500?  
My friends  
If you were a contestant on Jeopardy what would be your dream trivia category?  
Astrology  
Who in your life is going back to school?  
No one  
Do you own a cell phone? If yes, how long have you owned one?

**My eternal puppies** 2  
  
**Chris & Dan**  
  
  
8" of snow!!  
  
[View all \(4\) photos](#)

**GRIEF AND GRIEVING**  
Just Like the belly, there is no timeclock on grief and grieving. The process is as individual as the makeup of genes. Here is a venue for venting, for talking, for saying how YOU feel, even when all those around you cannot understand why you still morn.

**Most active members** 6  
 TJGal  
 Jo  
 Christina Ryan

# What do You Share, and with Whom?



# #1 Threat to Your Identity -- Phishing

---

- At Verizon we see an average of 40 phishing complaints per month.
- Many relate to fraudulent PayPal and banking websites designed to steal account credentials which can be used to steal credit card numbers or access bank accounts. Stolen credit card numbers are typically sold quickly on the black market.

# #1 Threat to Your Identity -- Phishing

---

- Many people unknowingly give away Internet service account and/or credit card data after receiving an email purportedly from their ISP, a bank or government agency.
- The scams can be seasonal (and clever) –
  - For example, phishing emails from the “IRS” and other government agencies claiming the email recipient had been chosen to receive an economic stimulus package

# #1 Threat to Your Identity -- Phishing

---

Common schemes targeting seniors according to the FBI:

- Health Insurance Frauds
  - Medical Equipment Fraud
  - Services Not Performed
  - Medicare Fraud
- Counterfeit Prescription Drugs
- Funeral and Cemetery Fraud
- Fraudulent "Anti-Aging" Products
- Telemarketing Fraud
- Investment Schemes

# Recent Phishing Scams

---

- **August 04, 2009** [Capital One Bank - Notification of restricted account access](#)
- **August 04, 2009** [Wachovia Bank - Dear Wachovia Customer](#)
- **August 04, 2009** [Bank of America - notification from: Bank Of America](#)
- **August 03, 2009** [Bank of America - Message from Customer Service](#)
- **August 03, 2009** [PayPal - Confirm refund request - Identity Verification](#)
- **August 03, 2009** [Bank of America - Customer Service Notification.](#)
- **August 03, 2009** [Bank of America - Safeguarding customer information](#)
- **August 03, 2009** [PayPal - Message from customer service: important notification](#)
- **August 03, 2009** [Bank of America - Bank of America customer service: official information](#)
- **August 03, 2009** [Bank of America - Update your account information](#)



# Sample Phishing Scam

**1**  
**From:** BestHomeLending (Besthome@lending.com)  
**Date:** **2** Friday, August 11, 2006 5 PM  
**To:** RodneyZ@email.com **3**  
**Subject:** New Financing Offer! Act Now Before Rates Go Up!

## **4** Refinancing Offer

**BestHomeLending** is pleased to offer you this exclusive opportunity to refinance your mortgage and *save hundreds of dollars* a month by simply transferring your existing loans into a new low fixed rate of only 5.75%. Use our [instant mortgage rate adjuster](#) to calculate how much you could be saving every month. **5**

This offer won't last long – **interest rates are expected to rise quickly and these rates can't last. We can only guarantee this exclusive rate for 3 more days!** **6** **7**

**8**  
Calculate Savings

**9**  
[Click here](#) to transfer your loan today – no closing costs, no hassles... just a lower interest rate to save you money.

Or call **BestHomeLending** at 1-800-TOP-LOAN between 9:00 am and 4:00 pm daily. **10**

### **Notice:**

This message was delivered to you as a service by **BestHomeLending**. We are committed to providing our customers with the best services available. **BestHomeLending** ensures your privacy and preferences. To View our privacy policies [click here](#). **11**

If at any time you wish to stop receiving service notices from **BestHomeLending** please [click here](#).

Please do not forward or reply to this message, it is generated by our automated system. Should you wish to reply to this email please contact our customer service representatives through [email](#), or call 555-1212 during regular banking hours. **12**

**BestHomeLending** USA 1321 Bank St. Carlsbad New Mexico 62309 **13**

Copyright 2001 © **BestHomeLending** All Rights Reserved.



# Take Control of Your Online Identity

---

- Use at least two search engines and search on yourself
- Run free credit reports --
  - By law, you have the right to a free credit report from each of the credit bureaus - TransUnion, Experian, and Equifax – each year.
- Establish your personal Internet privacy boundaries and let others know what they are
- Respect other's personal privacy
- You can't impose safety on others, but you can insist they not put you at risk

# Abuser's Mind Games

---

- If you feel threatened in any way, report it.
- The victim is never at 'fault'. Offenders bear complete responsibility for their actions.
- Scam artists rely on most users being too embarrassed to come forward.
- If the predator can convince you that the abuse was *your fault* you are much less likely to report it.

# Where do You Report Abuse?

---

- Local Police – even if the criminal claims to be from somewhere else
- National Center for Missing and Exploited Children – 1-800-THE-LOST – if the abuse includes the exploitation of a minor
- Better Business Bureau – if a business has acted fraudulently
- Online Provider – when abuse occurs through their tools
- Friends and Family - If the abuse impacts them (financial fraud) let them know

# What To Do About a Phishing Scam

---

What to do about Phishing and where to go for more information:

- Contact you ISP's abuse group (at Verizon our email address is: [abuse@verizon.net](mailto:abuse@verizon.net) or [security@verizon.net](mailto:security@verizon.net))
- Visit the FBI's website on phishing scams targeting seniors at:  
<http://www.fbi.gov/majcases/fraud/seniorsfam.htm>

# Parting Thoughts / Recommendations

---

- Use up-to-date security software to secure your computer and browser;
- Secure your wireless network;
- Use safe email addresses and passwords;
- Never click on a link in an email or provide your User ID, password or other sensitive account information in response to an email; and
- If you suspect you may have been the victim of fraud or abuse, report it.

# Parting Thoughts / Recommendations

---

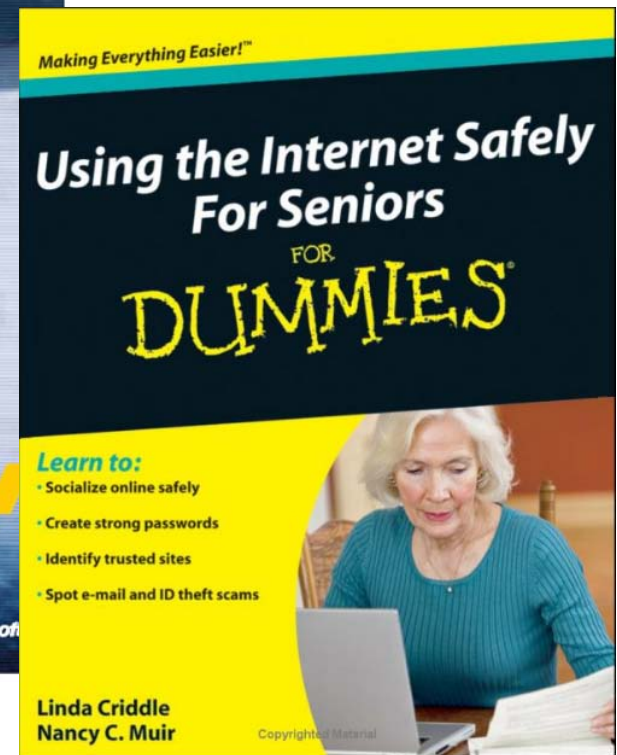
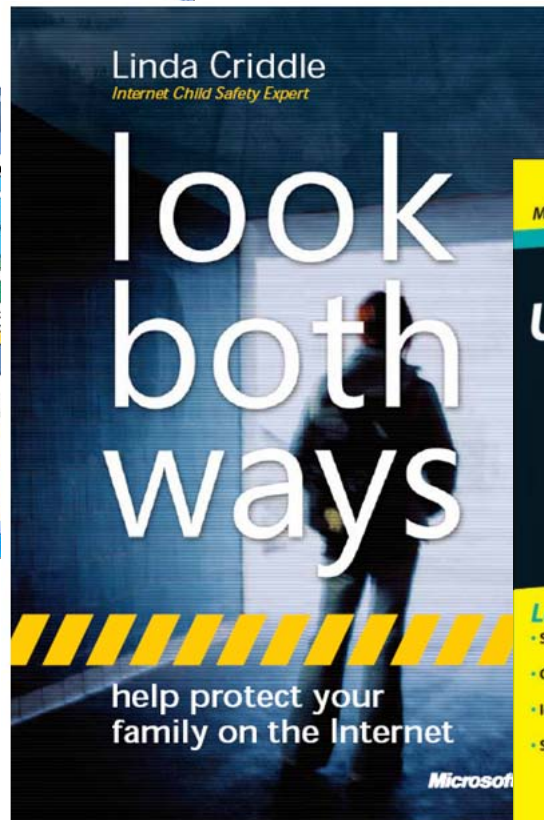
- Guard your information well. It is better to be rude than to be ripped off. Validate the site or person asking you for information before giving your information to anyone. If you still feel uneasy, simply say no.

# Learn More

The material for this presentation is provided by LOOKBOTHWAYS Inc. You can learn more about Internet safety on their website, and through their books.



[www.ilookbothways.com](http://www.ilookbothways.com)



---

# Questions?