

Home Computer Security: Protecting Yourself Online

Lori Ross O'Neil, Computer Scientist
Pacific Northwest National Laboratory
January 14, 2016



What we'll cover:

- ▶ It's not paranoia when they really are out to get you.
- ▶ Social networking – Oversharing at a global level.
- ▶ Keeping kids safe online
- ▶ Safe shopping – Not all deals are good
- ▶ Phishing – Will you take the bait?
- ▶ Malware – The dirty truth; its not just bad, its mean.
- ▶ Protection – Don't leave home without it.
- ▶ Oops, I think I did it again - Who to tell?
- ▶ Lori's list of tools



The National Lab System & PNNL



DOE's Mission

Discovering the solutions to power and secure America's future.



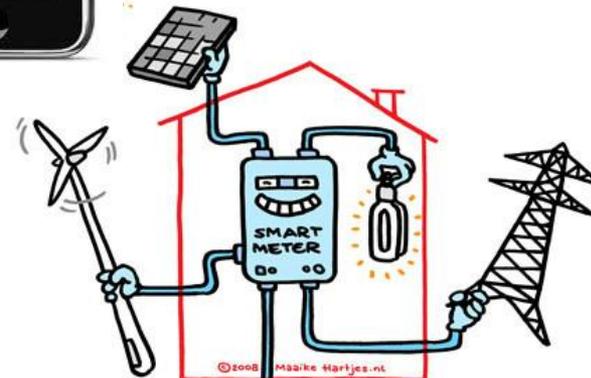
PNNL's Mission:

Transform the world through courageous discovery and innovation. It is our *vision* that PNNL science and technology inspires and enables the world to live prosperously, safely, and securely. www.pnnl.gov



Pacific Northwest
NATIONAL LABORATORY

What is a computer?



If it seems like someone is watching you...
They are.

Web | MSN | Images | Video | News | Maps | Shopping

bing Web Search

Make Y! your home

YAHOO! NEWS

new

Saturday, January

YAHOO! SITES

- Autos
- Dating
- Finance (Dow ↑)
- Flickr
- Games
- Horoscopes
- Jobs
- Mail
- Messenger

msn

Tracker Blocker

Nice! You've blocked **30532** trackers.

Daily # trackers blocked

3200

2400

1600

800

0

Oct 12 Oct 30 Nov 17 Dec 5 Dec 23

Preventir

33acro

[x+1] Mortgage rates

Acerno

AdChoices

Adap.T

Adaptiv

Learn more
blocker

NETFLI

Netflix FREE for

TV episodes and m

rate Kid dad want...

m Arnold baby

ALWAYS SUNNY IN PHILADELPHIA

Northwest
LABORATORY

There is no free lunch.



- ▶ Using services on free sites, means you are the content.
- ▶ By using the site you are agreeing to let them monitor and even sell your actions and data.
- ▶ Know the site's privacy policy and opt-out.
- ▶ Give out your personal information sparingly, much is already online (Benton county property tax, registered voters, etc.)

The image shows two overlapping screenshots of privacy policy pages. The top screenshot is from Google, displaying the Google logo and the text 'Policies & Principles'. Below the logo are navigation links for 'Overview', 'Privacy', and 'Terms of Service'. The bottom screenshot is from Yahoo!, displaying the 'YAHOO! PRIVACY' logo and a search bar. Below the logo are buttons for 'Home', 'Products', 'Topics', and 'Privacy Tools'.

The image shows a screenshot of the Facebook 'Privacy Settings and Tools' page. The page title is 'Privacy Settings and Tools'. Under the heading 'Who can see my stuff?', there are two settings. The first setting is 'Who can see your future posts?' with the value 'Only Me' circled in red. The second setting is 'Review all your posts and things you're tagged in' with the option 'Use Activity Log'.

Setting up online accounts:

Create a list of info for online accounts/forms

My Online Avatar:

- ▶ Avatar Name: Lara Craft
- ▶ Avatar Userid: LaraTheCrafter
- ▶ Avatar Birth City: Hogsmeade
- ▶ Avatar School: Hogwarts
- ▶ Avatar Pet's Name: AragogTheDog
- ▶ Avatar First Car: Purple
- ▶ Avatar Spouse Meet: Jup!t3r
- ▶ Avatar First Job: Queen
- ▶ Avatar Birth Date:
- ▶ Avatar Email address:
- ▶ Avatar IM Address:
- ▶ Avatar Mother's Maiden Name:
 - Sarah-Palin

The screenshot shows a web browser window with the URL <https://auth.dhs.gov/registration/Registration?source=HSIN&action=EUSbe2g8x9ez>. The browser tabs include "HSIN Account Registration", "Balch & Bingham LLP - Electri...", and "google.com". The page title is "HSIN Account Registration". The form includes a "Password" field and a "Confirm Password" field, both with masked characters. Below these fields is a section titled "Password Reset Questions" with the subtitle "In the event you forget or need to change your password, these questions will be". There are four security questions and their corresponding answer fields. The first question is "What is your mother's maiden name?" and the first answer field is highlighted in blue. The second question is "What is the city of your birth?". The third question is "What is the name of your pet?". The fourth question is "What is your favorite color?". The first answer field for the second question is "In what city and country do you want to retire?". The second answer field for the second question is "What was your high school mascot?". The third answer field for the second question is "What year did you graduate from High School?". The fourth answer field for the second question is "What is the name of the first school you attended?". The first answer field for the third question is "What was the name of your elementary / primary school?". The second answer field for the third question is "What is the name of the company of your first job?". The third answer field for the third question is "What was your favorite place to visit as a child?". The fourth answer field for the third question is "What is your spouse's mother's maiden name?". The first answer field for the fourth question is "In what city or town was your first job?". At the bottom of the form, there is a "Passcode Settings" section with a question mark icon.

Keeping kids (and seniors) safe online



- ▶ Have open discussions about threats in DL (digital life) and RL (real life).
- ▶ Develop a family Technology Code of Conduct and rules that everyone agrees to.
- ▶ Use a central family charging location and put devices there at night and during meals.
- ▶ Dedicate technology for their use that has parent set controls, filtering and monitoring.



Our Family Technology Code of Conduct

I promise: I will always keep my identity private. I will never share personal information such as my name, mailing address, phone number, and name of my school or other information that could be used to identify me online. I will also not reveal any personal information about my friends or family members. I will never send a picture or any other media file with out first checking with my parents or guardian.

Signature of student: _____ Date: _____

Signature of parent: _____ Date: _____

Keeping kids (and seniors) safe online, continued

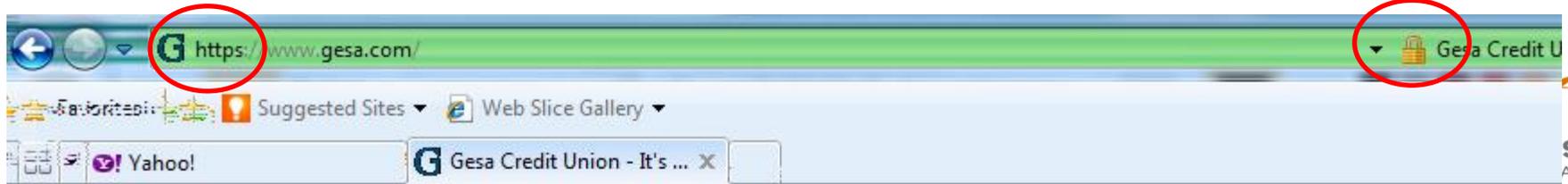


- ▶ Kids with smart phones need to keep them charged, respond promptly to parents and use responsibly.
- ▶ Use shared family accounts for email, games, etc. (Apple FamilySharing)
- ▶ “Friend” your kids and play online with them.
- ▶ Do random device checks of use, history, chat, contacts, pictures, etc.
- ▶ Parents manage admin accounts and know all kid’s accounts and passwords.
- ▶ Don’t post anything you don’t want seen *forever*.
- ▶ Kids: *Teach parents about technology.*

Safe Online Shopping and Banking



- ▶ Shop at reputable, well-known sites.
- ▶ Never shop online with debit card or checking account.
- ▶ Use third-party financial pay services.
- ▶ Don't store payment info on shopping site
- ▶ Turn on alerts/notifications for payments or banking.
- ▶ Dedicate one credit card for online shopping and another for in person shopping.
- ▶ Ensure the site has a lock icon and https in address.



What is Phishing?

Messages that look legit but are malicious



Online Banking Alert

Need additional
up to the minute
account
information?
[Sign In >>](#)

Change of Email Address

Your primary e-mail address for

Did You Know? You can change
[Online Banking](#) and click on the



On

[Sign In](#)

<http://boa.com-stz.info/boa.ru>

alert will not accept replies. If you
comments, please [sign in to Online](#)

Enter Online ID:

(6 - 32 characters)

Enter Password

Save this Online ID ([How does this work?](#))

Not using O
[Enroll now](#)
for Online B

[Learn more](#)
about Onlin

[Service Ac](#)

<https://www.bankofamerica.com>

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#) 
© 2004 Bank of America Corporation. All rights reserved

[Reset passcode](#)

[Forgot or need help with your ID?](#)

 **Secure Area**

[Home](#) • [Locations](#) • [Contact Us](#) • [Help](#) • [Sign in](#) • [Site Map](#)
[Personal Finance](#) • [Small Business](#) • [Corporate & Institutional](#)
[About the Bank](#) • [In the Community](#) • [Finance Tools & Planning](#) • [Privacy & Security](#)

Or Phishing looks like this – *So do this!*

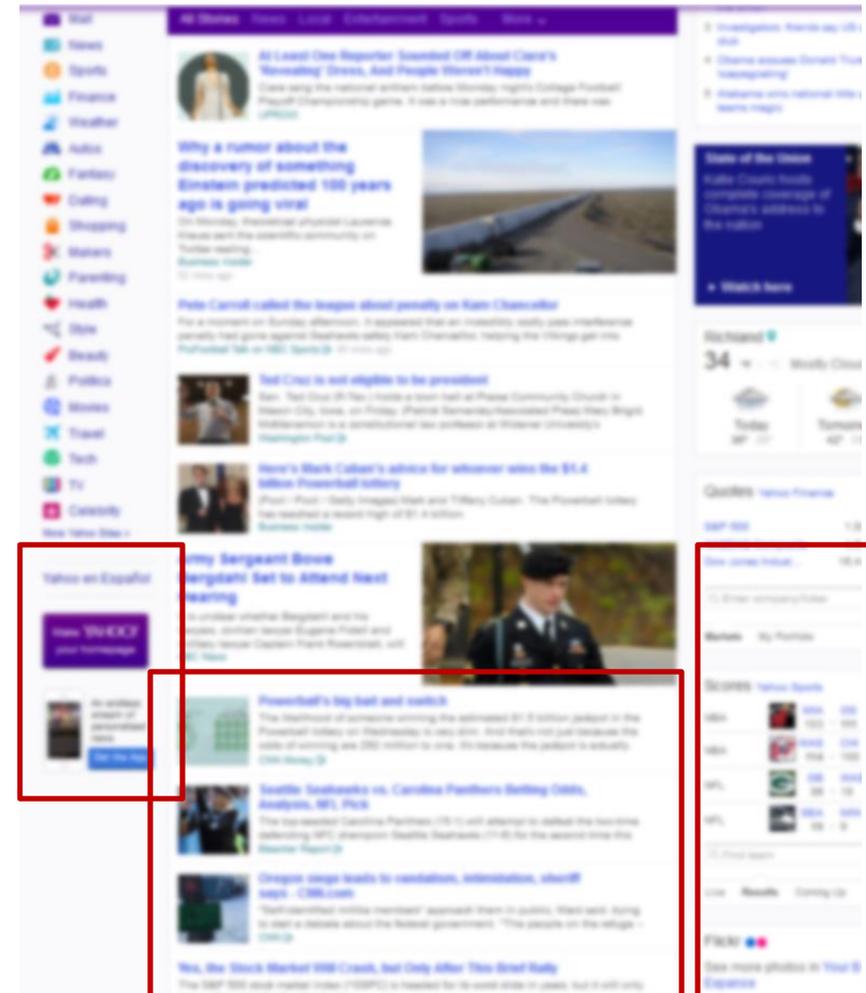


- ▶ Only click on links or open attachments you are expecting and from people you know.
- ▶ Rather than clicking on the link, type the URL yourself or use your bookmark.
- ▶ If it seems suspicious, call to verify.
- ▶ Don't send personal information via email or text.
- ▶ Have multiple accounts (work, social, etc).
- ▶ Only enter info via safe, trusted web sites. (https)

Malware infections can occur while online

Malicious Software controls and harms systems

- ▶ Malware can be annoying pop-ups, ransomware, destroy files or controls your browser.
- ▶ Even well known sites can have links to less reputable sites, leading to malware infections.
- ▶ Infections can occur during popular searches.
- ▶ Read carefully before clicking, especially on ads.



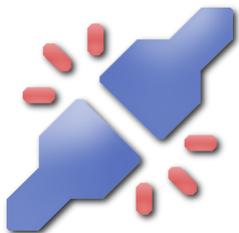
Preventing and recovering from malware

To prevent malware infections:

- ▶ Stick to reputable sites and notice when browsing leads you away.
- ▶ Use an ad blocker

What to do if you are infected:

- ▶ Disconnect from the internet
- ▶ Use software to scan and remove malware immediately.
- ▶ Use an anti-malware product for real-time protection.



How do I protect my systems from bad stuff?

For all digital devices (computers, phones, tablets):

- ▶ Keep operating system and applications current, auto-update. Allow built-in security and privacy.
- ▶ Use anti-malware software.
- ▶ Back up your systems automatically.
- ▶ Set your systems to go to the right web site.
- ▶ Use public wireless cautiously.
- ▶ Use a firewall – on your computer, wireless router and your ISP modem. Should be enabled by default.
- ▶ Never run as “home” or “admin”. Use unprivileged accounts.



Where to get help...



If you suspect you have been the victim of a scam, identify theft or crime you should contact:

- ▶ Your local police department
- ▶ FBI Internet Crime Complaint Center (IFCC) www.ic3.gov
- ▶ Federal Trade Commission www.ftc.gov
- ▶ 3 major credit bureaus to help protect financial information from identity theft. (Experian, Equifax, TransUnion)
- ▶ Be sure to report to the real site as well, such as PayPal, etc.

For more info:

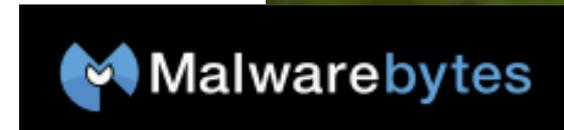
- ▶ FBI Social Media Config www.etsu.edu/oit/helpdesk/smcards.aspx
- ▶ US-CERT www.us-cert.gov
- ▶ Microsoft Security for Home Use www.microsoft.com/security
- ▶ OnGuard Online onguardonline.gov
- ▶ Online Promise www.safekids.com/kids-rules-for-online-safety

Security Tools – Free and low cost

*Lori's top picks**



- ▶ Ad Blocker – Adblock browser add-on or extension
- ▶ Web Site Verification – OpenDNS
 - www.opendns.com/home-internet-security
- ▶ Password & Account manager - Blur
 - dnt.abine.com
- ▶ Malware Protection & Recovery
 - Avast - avast.com
 - AVG - avg.com
 - Malwarebytes - malwarebytes.org
- ▶ Kid Monitoring
 - Teen Safe teensafe.com
 - My Mobile Watchdog mymobilewatchdog.com
 - WebWatcher webwatcher.com



**These are my picks alone based on experience and recommendations of my peers. This is in no way an endorsement by me or PNNL.*

Pacific Northwest
NATIONAL LABORATORY

Questions? Answers?

Final Thoughts:



- ▶ This presentation will be available at:
 - regionalloutreach.pnnl.gov/seminars

1. Make online safety a habit.
2. Develop a more secure digital life, gradually.
3. Use a multi-layered approach to security –
 - Firewalls, system updates, strong passwords are the equivalent of walls, moats and archers.
4. Be active online with those you care about.
5. Advocate online safety.

