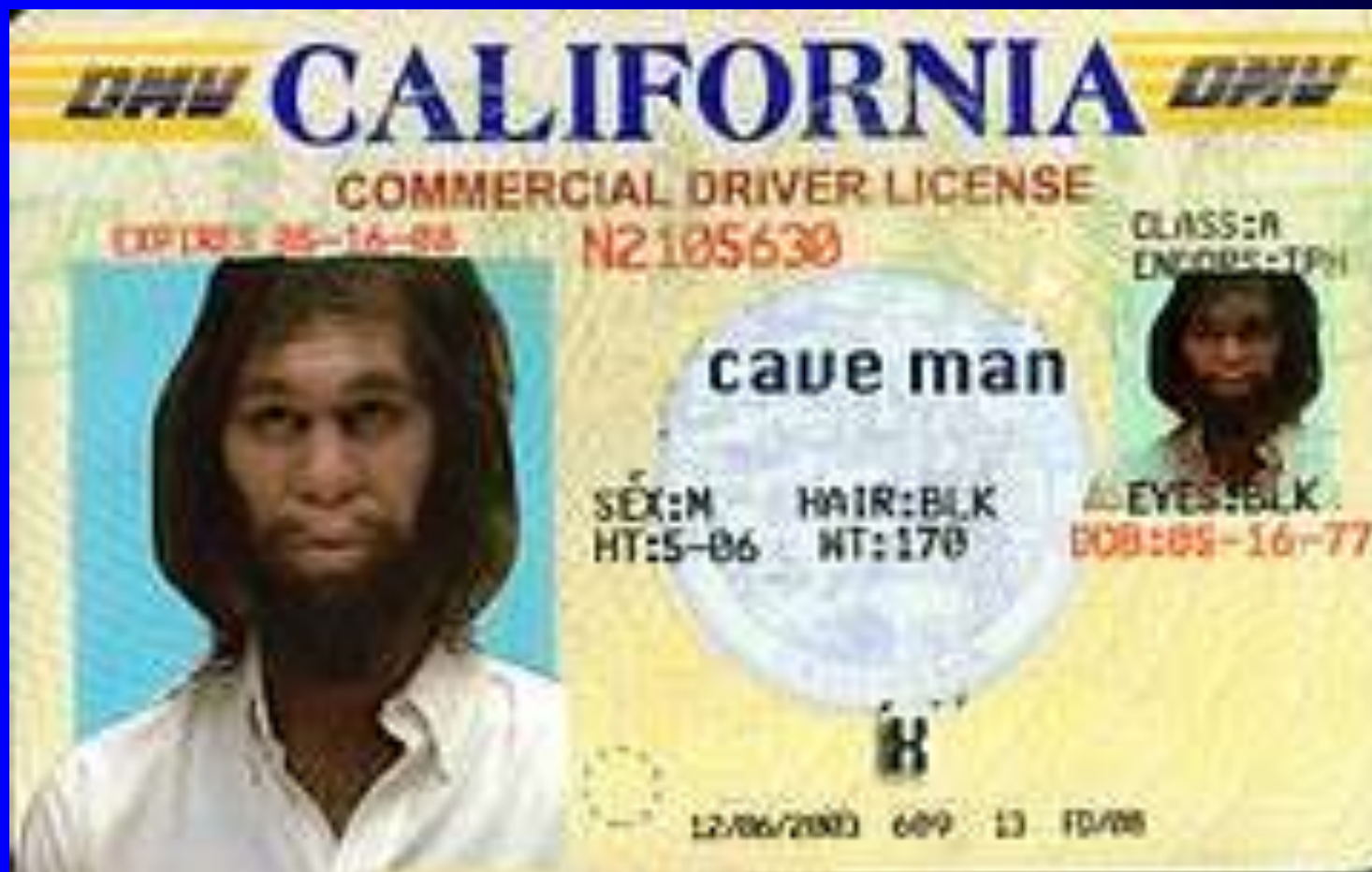


Detecting & Protecting Your Digital Footprint at Work and Home: ID Theft and You!: A LibraryLinkNJ Webinar

By Professor-Librarian Robert J. Lackie / 9-20-2011



Objectives

- Analyze ID safety issues, at work and home—and in between (on the road)
- Apply safeguards and remove unwanted information
- Connect to and retrieve additional tools and resources

*It's all about ... **convenience vs. safety***

Poll #1

ID theft/fraud victims are in this webinar, in your family, or at your work; how many do you know that have dealt with....

Q1: mail (work or home) theft?

Q2: stolen wallet or purse?

Q3: credit card fraud?

Q4: ATM skimming or debit card fraud?

Q5: computer/smartphone/email hacks?

Quiz #1

[https://www.privacyrights.org/
itrc-quiz1.htm](https://www.privacyrights.org/itrc-quiz1.htm)



Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

[Home](#) [Why Privacy](#) [About Us](#) [Fact Sheets](#) [Latest Issues](#) [Speeches & Testimony](#)

Browse Privacy Topics

[Privacy Basics](#)

[Background Checks & Workplace](#)

[Banking & Finance](#)

[Credit & Credit Reports](#)

[Debt Collection](#)

[Education](#)

Identity Theft IQ Test

 [Send to Printer](#)

Copyright © 2000-2011
Privacy Rights Clearinghouse / UCAN
Posted December 1, 2000
Revised June 2009

Are You at Risk for Identity Theft? Test Your "Identity Quotient"

Tip #1

Shred with at least a crosscut shredder (but a ***micro*** shredder is even better) all pieces of mail that contain any personal information before throwing them in the trash, at the library, at home, on the road

Tip #2

Place outgoing mail and retrieve incoming mail via a locking mailbox or official Postal Service box, not the community office bin or the mailbox in front of your house

Tip #3

Inventory/photocopy/scan what is in your wallet/purse and place that copy (back & front of cards) in a locked cabinet—if your wallet/purse is stolen, you have all the info you need—and remove that SSN card now!!

Tip #4

Use a virtual credit card number (available through most banks) for online purchases, rather than your “real” credit card—connected to your card, the virtual number can be set up to only be used once, for that one online purchase, or a few

Tip #5

Keep an eye on your credit or debit card when you are paying for something—don't allow it to disappear out of your sight (skimming of your card could occur)

Tip #6

Use your credit card instead of your
debit card—better protection,
different laws
(Fair Credit Billing Act
vs.
Electronic Funds Transfer Act)

Tip #7

Cover the ATM keypad from prying eyes and cameras with one hand while you enter your PIN—and use the one at your bank instead of stand-alone ATMs (skimmers are everywhere in NJ!!)

Tip #8

Avoid sending sensitive info through email and web—look for the security clues on web sites, and the letters at the beginning of the address bar at the top of the screen should change from “*http*” to “*https*” when the site is secure

Poll #2

Username & Passwords:

How many of you, honestly, do this?:

Q1: Auto save either for any of your accounts?

Q2: Use same one(s) for many of your accounts?

Q3: Make passwords 8+ characters long?

Q4: Ensure passwords contain lowercase, uppercase, numbers, and symbols?

Tip #9

Keep your passwords **safe AND strong**, using different ones for different sites—and try updating your passwords to passphrases, changing them a few times a year, verifying strength:

www.passwordmeter.com

Tip #10

Clear private data from all browsers (i.e., Firefox): delete temporary files, browsing history, cookies, cache, saved form information/passwords, and *especially* when using a public computer or kiosk at a library, hotel, airport, coffee shop, etc.—and then shut down your browser.

Tip #11

Update your browsers, *right after webinar!*

“It looks like you may be using an outdated browser with known security issues. Please take a moment to download a safer browser. Click these common browsers (IE, Firefox, etc.) for update instructions:”

From PayPal, visit their ‘*Security & Protection*’ link at top, and then ‘*Hardware and Software Security*’ link at the bottom:

<https://www.paypal.com>

Tip #12

Lock down your mobile devices!: *phone contacts, private e-mail, chats, financial data, saved ID's and password, etc*—basically, **your life is in there!**

Consider password protection, or even [LoJack](#) or [McAfee](#) (can also remotely lock down/freeze device or erase sensitive files or data if it is stolen)

Tip #13

Remove some of your personal info on ‘*notable social networking sites*’—see category 1 of my site “Personal Profiles and Other Publicly Available Information” for listings/descriptions:

www.kn.att.com/wired/fil/pages/liststudentpe3.html#cat1

Tip #14

Locate & remove your personal listing or some info on ‘*notable personal information search engines*’—see category 2 of my site “Personal Profiles and Other Publicly Available Information”:

www.kn.att.com/wired/fil/pages/liststudentpe3.html#cat2

Tip #15

Opt out with marketing companies of future credit card solicitations by calling (888) 5OPTOUT or visiting www.optoutprescreen.com

Tip #16

Reduce telemarketing calls at home with the National Do Not Call Registry—to get more information, visit www.donotcall.gov, or call 1-888-382-1222 from the phone number you want to register

Tip #17

Opt out with the Direct Marketing Association (DMA) to receive less unsolicited commercial mail AND email from many national companies; **visit**
www.dmachoice.org


Tip #18

Never respond to an unsolicited email from your financial or medical organizations, and don't unsubscribe from these emails either—don't click on any links within, and don't even open the email itself. Just delete it

Tip #19

Learn to distinguish real from fake emails

Find it. Trust it. Know it. Instantly!
The Iconix® Truemark® service makes it easy.




Without eMail ID With eMail ID


Inbox

View: All Messages [Lock] [Mark] [Move]


Sender

 eBay your shipping address


Michael Purcell weekend?

 Wells Fargo statement available


Dutch Hancock Do you need help fixing your fence?

 PayPal Receipt for your payment to Fastball.com

Truemark icons show you which emails are real!



Try Iconix® eMail ID – find and trust messages you care about.

Download for free: 

For use with:
Windows Live™ Hotmail®
AOL® webmail, Yahoo!® Mail
Outlook® Express, Gmail™
and many others!

www.iconix.com

@Copyright 2011, Robert J. Lackie,
Rider University Libraries

Quiz #2

www.consumerreports.org

Phishing Trip

Millions of consumers get taken in every year by “phishing” scams, e-mails that appear to be from a bank or other institution, but are actually cons designed to separate you from your money. To help sharpen your skills at recognizing such scams, try this interactive quiz.

Click the **Next** button below to see a series of 12 screen shots of actual e-mails, both fraudulent and legitimate, from which we’ve removed the names and addresses. For each, click to tell us whether you think it’s REAL or FAKE. We’ll tell you whether you were right, why, and show you how accurate you’ve been overall. (Note: We won’t retain any record of this quiz after you’ve completed it.)

Good luck! Here’s hoping you avoid getting “hooked.”

Next >



Tip #20

Review your credit reports (you can get a free one each year from each of the three credit reporting agencies, and if you stagger requests, you can get a different one every four months):

<https://www.annualcreditreport.com>

Everybody: order 1 or all 3 today!

You are Nervous, and Want More Help/Advice??



Identify Suspicious Activity

www.ftc.gov/bcp/edu/microsites/idtheft/consumers/detect.html

Stay alert for the signs of identity theft, like:

- accounts you didn't open and debts on your accounts that you can't explain.
- fraudulent or inaccurate information on your credit reports, including accounts and personal information, like your Social Security number, address(es), name or initials, and employers.
- failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- receiving credit cards that you didn't apply for.
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

It's Your Digital Footprint!

Explore in-depth pertinent
*'Notable Online Identity/Privacy
Information Resources'* sites —
yes, again, see section 3 of my
site “Personal Profiles and Other
Publicly Available Information”:

[www.kn.att.com/wired/fil/pages/list
studentpe3.html#cat3](http://www.kn.att.com/wired/fil/pages/liststudentpe3.html#cat3)

ID Theft Protection Services??

<https://www.privacyrights.org/fs/fs33-CreditMonitoring.htm> and then visit

www.nextadvisor.com

Overview | Compare All Services | [FAQ](#) | [Blog](#) Search NextAdvisor.com
Google™ Custom Search

Identity Theft Protection Reviews & Prices

Identity theft is the fastest growing crime in the U.S., with over nine million victims each year. Just being careful isn't enough to protect your identity. If you are serious about preventing identity theft, sign up for one of our recommended identity theft prevention services. They all provide daily monitoring of the information that is most often compromised by identity thieves. Our top-rated services combine multiple types of monitoring, such as credit reports, public records, credit cards, and Social Security. Some also include software to protect your computer and even throw in access to your credit scores. Have more questions about identity theft and which service might be best for you? [Visit our FAQs.](#)

Identity Theft Protection Reviews & Prices						Updated 05-06-2011
Service Name / Rating:	Price:	Fraud Monitoring:	ID Theft Insurance/ Guarantee:	Reports Delivered:	Computer Security:	Bottom Line:
 IDENTITY GUARD Total Protection ★★★★★ Go To Site Read Full Review	Free 30-day trial; \$14.99/mo (after our limited time discount)	Monitors 3-bureau credit report, credit cards, public records, Social Security number, applications, Internet security	\$1,000,000 insurance	All 3 bureau credit scores and a public record report each quarter	ZoneAlarm Internet security suite; anti-keylogging software	Most complete ID theft protection service; full credit report monitoring; free Internet security suite; 18% discount & free 30-day trial
 TrustedID™ 1-800-234-6611 ★★★★★ Go To Site Read Full Review	Free 14-day trial & 15% discount; \$7.01/mo w/ annual prepay	Monitors credit cards, public records, Social Security number, bank accounts, medical records	\$1,000,000 warranty	One 3-bureau credit report each year	Anti-spyware protection	Best value, especially for families; free 14-day trial & 15% discount; to sign up over the phone, call 800-234-6611
 LifeLock. ★★★★★ Go To Site Read Full Review	Free 30-day trial; \$8.25/mo (w/ annual prepay)	Monitors applications, credit cards, Social Security number, driver's license, address change	\$1,000,000 guarantee	One 3-bureau credit report each year	None	Strong overall value; 10% discount & free 30-day trial

Free 29-page Handout

<http://library.rider.edu/~rlackie/idtheft/RU2011.pdf>



CENTER FOR BUSINESS FORENSICS
College of Business Administration

Identity Theft: What You Need To Know

Organizer, Contributor, and Panel Moderator:
Dr. J. Drew Procaccino
Associate Professor, Department of Computer Information Systems, Rider University

Contributor and Panelist:
Prof. Robert J. Lackie
Professor-Librarian, Franklin F. Moore Library, Rider University

ID theft has taken place?: *Advice/Step #1*

Place a fraud alert on your credit reports & review them: call

TransUnion: 1-800-680-7289;

www.transunion.com/

Fraud Victim Assistance Division,

P.O. Box 6790, Fullerton, CA

92834-6790

ID theft has taken place?: *Advice/Step #2*

Close only the accounts that you know (or believe) have been tampered with or opened fraudulently, speak with someone in the security or fraud department of each company, and follow up in writing, certified mail

ID theft has taken place?: *Advice/Step #3*

File a complaint with the FTC using the [online complaint form](#); or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580

ID theft has taken place?: *Advice/Step #4*

File a report (in person if possible) with local police or the police in the community where the identity theft took place, and bring a printed copy of your FTC ID Theft Complaint form, your cover letter, and copies of supporting docs

“Questions

AND

Answers!”

Goin' Phishin' Video / Conclusion

www.consumerreports.org



@Copyright 2011, Robert J. Lackie,
Rider University Libraries

PowerPoint Presentation Slides:

<http://library.rider.edu/~rlackie/idtheft/protectingNJ2011.ppt>

Robert Lackie
rlackie@rider.edu

Robert J. Lackie is a Professor-Librarian at Rider University in New Jersey, where he co-leads the course-integrated Library Instruction Program. A frequent presenter at local, state, and national library, education, and technology conferences, Professor Lackie has presented over 500 workshops and seminars around the United States, and he has been published within various professional and scholarly works. His co-edited book, *Teaching Generation M: A Handbook for Librarians and Educators*, was published in 2009. See the URL below for the book description. If discount order [\[CITE\]](http://library.rider.edu/~rlackie/Bowman-Lackie_GenM.pdf)

Curriculum Vitae
Short Bio and Current Seminars/Workshops
Other online materials

StatCrunch JotEasy



Thank you for attending!