

Combating Identity Theft: Tips to Reduce Your Cybersecurity Risks

October 20, 2015

Current Cyber Threat

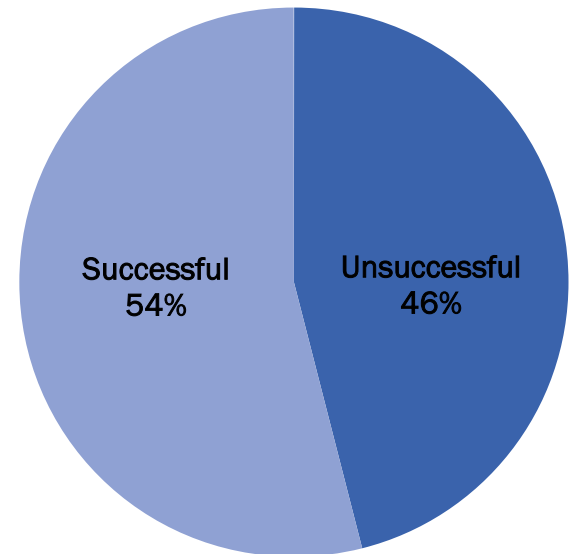
- Cyber criminals are not only targeting businesses, but individuals
- Stolen personally identifiable information (PII) is not one-time use
 - Data is pooled
 - Individual profiles created and sold

Examples:

- Tax Fraud
- Health Care Fraud
- Spear-Phishing
- Individual Account Compromise

Tax Fraud

- Cyberattacks against the IRS larger than expected¹
 - Over 610,000 attempted account breaches, 330,000 were successfully breached
 - **271%** more attempts
 - **289%** more accounts breached
 - **252%** more unsuccessful attempts than originally estimated in May 2015



Local Examples:

- Archdiocese of Portland
- Archdiocese of Seattle

¹ John D. McKinnon and Lara Saunders, "IRS Says Cyberattacks More Extensive Than Previously Reported," <http://www.wsj.com/articles/irs-says-cyberattacks-more-extensive-than-previously-reported-1439834639> (Aug. 17 2015).

² Brent Hunsberger, "Oregon investigating complaints about the Archdiocese of Portland's handling of ID theft," http://www.oregonlive.com/finance/index.ssf/2014/05/oregon_investigating_complaint.html (May 3, 2014).

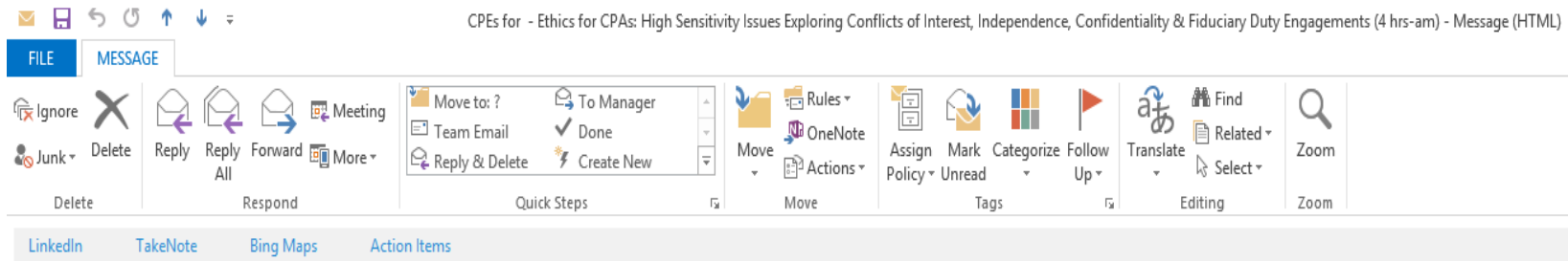
Health Care Fraud

- Healthcare information is more expensive in the black market than financial data¹:
 - Credit card information = **\$1**
 - Partial health insurance credential = **\$20**
 - Full profile, including health insurance information = **\$1,000**
- Why is it so valuable?
 - Used to obtain medical care
 - Fraudulent billing of insurance, Medicare, and Medicaid

Spear-Phishing Still Effective in 2015

- **23%** of included recipients were found to have opened phishing messages
- **11%** clicked on corresponding attachments
- **90%** chance that at least one person will fall victim to their attack (out of 10 emails received)

Spear-Phishing Email – Indicators



Dear CPE Participant:

Thank you for attending the Ethics for CPAs: High Sensitivity Issues Exploring Conflicts of Interest, Independence, Confidentiality & Fiduciary Duty Engagements (4 hrs-am), at:

Embassy Suites Hotel Washington Sq
9000 SW Washington Sq Rd
Tiger, Oregon

Misspelled words

https://www.orcpa.ru/professional_development/educational_catalog/09331-ethics_for_cpas_high_sensitivity_issues_exploring_conflicts_of_interest_independence_confidentiality_fiduciary_duty_engagements_4_hrs-am/
Click to follow link

When you mouse-over the survey link, the URL is **NOT** to [oscpa.org](https://www.oscpa.org), but rather to [orcpa.ru](https://www.orcpa.ru)—a Russian domain

In order to receive your CPE credits, please complete the following survey at the follow

[Survey for Ethics for CPAs: High Sensitivity Issues Exploring Conflicts of Interest, Independence, Confidentiality & Fiduciary Duty Engagements](#)

You will receive an e-certificate for 4 credits once you complete the survey.

We hope you enjoyed the CPE session.

All content herein copyright Oregon Society of CPAs. All Rights reserved.

If you have questions or comments, please contact us.

Mailing: PO Box 4555, Beaverton, OR 97076-4555





Location: 10206 SW Laurel St., Beaverton, OR 97005-3209 | Main: 503-641-7200 | Fax: 503-626-2942

Real information to make the phishing email seem like it originates from the real organization

Individual Account Compromise

From iCloud to individual financial accounts, hackers are targeting high net worth individuals.

Some tips to remember:

1. Secure online accounts 
2. Secure social media   
3. Restrict access to information

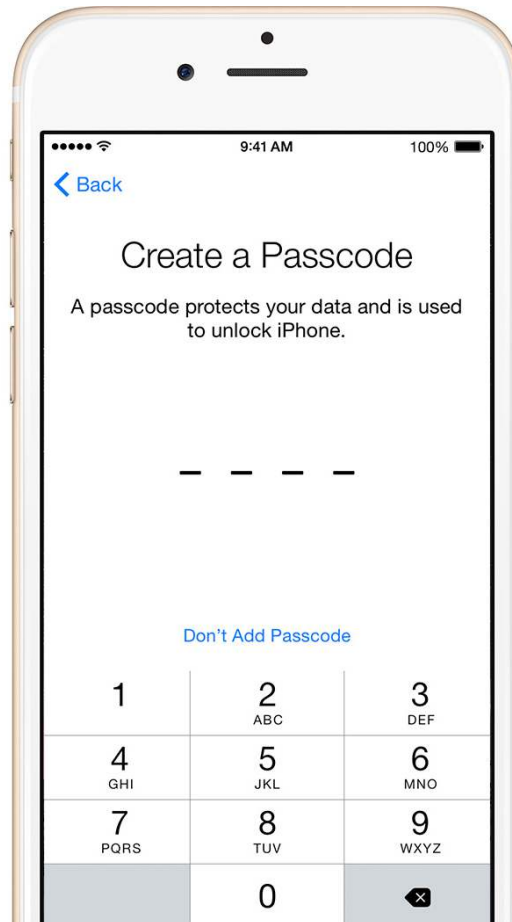
Recognize These High Risk Behaviors?

- Using **unsecure public Wi-Fi Networks** with sensitive websites



Recognize These High Risk Behaviors?

- No **password** on mobile devices



Recognize These High Risk Behaviors?

- Using the **same password** across multiple accounts



Recognize These High Risk Behaviors?

- **Oversharing on social media** (posting photos with sensitive information included)



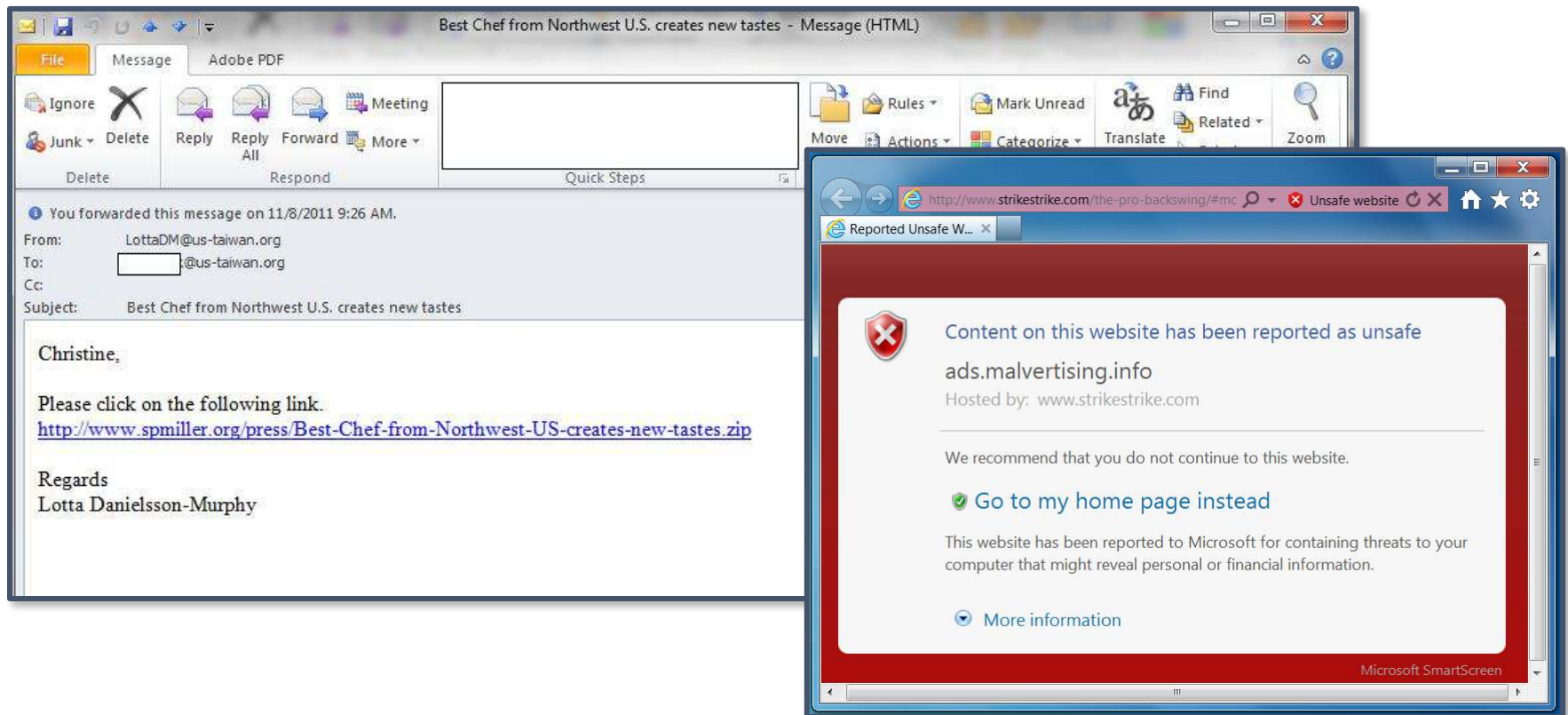
Recognize These High Risk Behaviors?

- **Not shredding sensitive documents** before throwing them in the trash



Recognize These High Risk Behaviors?

- Surfing **suspicious internet sites** or **clicking on links and attachments** from unverified sources



Top 5 Tips for Securing Your Personal Info

- 1. Use a password on your mobile device** (phone, tablet, laptop, etc.) and be diligent when disposing of it
- 2. Use wireless networks cautiously** (Virtual Private Network (VPN), encryption keys, etc.)
- 3. Monitor your credit reports**
 - a) Consider implementing a “**security freeze**” with the credit bureaus
 - b) Make use of the **free annual credit report** from www.annualcreditreport.com
 - c) Consider **Identity Theft Insurance**
- 4. Be wary of phishing emails;** do not click on a link or download files from unknown sources
- 5. Be mindful of what you disclose on social media** (e.g. full birthdate, date of graduation, favorite color, pictures, location, live posting of information, etc.—they may be used as a security question)

The Connected Consumer

Who's listening and what are they doing with your data?



Are they spying on you?

Internet of Things (Connected):

- LED light bulbs
- Cars
- Thermostats
- Baby monitors
- Smart TVs

Questions?



Miguel San Mateo
Principal
503.802.8644
msanmateo@perkinscas.com



Ryan McLean
Manager
503.221.7545
rmclean@perkinscas.com

Thank You!

Appendix A - Fighting Tax Fraud

- Request a 90 day fraud alert on your Experian file. Experian should notify the other credit reporting agencies.
- File a report with the FTC. Use the FTC Report as a theft affidavit for police reports, etc.
- Request your free credit report form the credit reporting agencies. They should be free once you file the fraud alert.
- Place a security freeze on your file with the credit reporting bureaus.
- File a police report with local law enforcement, using your FTC affidavit.
- Notify your bank, credit card companies, and other financial institutions, and even your utility companies.
- Monitor your bank, credit card, and other financial statements for other suspicious activity.
- Contact the IRS and your state's Department of Revenue (state taxation body) and file an Identity Theft Form 14039. Request an Identity Theft Protection PIN.¹

Appendix B - Mitigating Health Care Fraud

- Be very cautious of who you provide your medical insurance information to.
- If someone calls requesting your information, consider calling the company back using the number on the back of your card instead of providing information to the caller.
- Review and monitor your Explanation of Benefits (EOB) for any suspicious charges. Follow-up as necessary.
- Shred any paper prescription labels, expired medical insurance cards, etc.