LIST OF REFERENCES

[1] Abu-Nimeh, S., Nappa, D., Wang, X., and Nair, S. A comparison of machine learning techniques for phishing detection. In *eCrime '07: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (New York, NY, USA, 2007), ACM, pp. 60–69.

[2] Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., and Roinestad, H. Phishing IQ tests measure fear, not ability. *Usable Security (USEC'07)* (2007). `http://usablesecurity.org/papers/anandpara.pdf`.

[3] Anderson, J. R. *Rules of the Mind.* Lawrence Erlbaum Associates, Inc., 1993.

[4] Anderson, R., and Moore, T. The economics of information security. *Science 314*, 5799 (2006), 610–613.

[5] Andy Patrizio. Symantec readies phishing protection software, august 7, 2006. visited jan 1, 2009. `http://www.smallbusinesscomputing.com/news/article.php/3624991`.

[6] Anti-Phishing Working Group. Anti-phishing Best Practices Recommendations for Registrars. Report, 2008. `http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf`.

[7] Anti-Phishing Working Group. Global Phishing Survey: Trends and Domain name use in 2H 2008. Report, 2008. `http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf`.

[8] Anti-Phishing Working Group. What to Do If Your Website Has Been Hacked by Phishers. Report, 2008. `http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf`.

[9] AOL Press Release. It's 3 a.m. – are you checking your email again? july 30, 2008. visited jan 1, 2009. `http://corp.aol.com/press-releases/2008/07/it-s-3-am-are-you-checking-your-email-a`

[10] Apple Inc. . New features in safari. `http://www.apple.com/safari/features.html#security`.

[11] ASSOCIATED BANK-CORP v. EARTHLINK, INC. Memorandum and order, 05-c-0233-s. http://www.iplawobserver.com/cases/2005-09-14_Associated_Banc_Corp_CDA_Secti

[12] Avantgarde. Time to Live on the Network. Tech. rep., Avantgarde, 2004. http://www.avantgarde.com/xxxxttln.pdf.

[13] Blais, A.-R., and Weber, E. U. A domain-specific risk-taking (dospert) scale for adult populations. *Judgment and Decision Making 1*, 1 (2006), 33–47 KW –.

[14] Calman, C. Bigger phish to fry: California's antiphishing statute and its potential imposition of secondary liability on internet service providers. *Richmond Journal of Law and Technology XIII*, 1 (2006).

[15] Cavusoglu, H., and Raghunathan, S. Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches. *Decision Analysis 1*, 3 (2004), 131–148.

[16] Chou, N., Ledesma, R., Teraguchi, Y., and Mitchell, J. C. Client-side defense against web-based identity theft. In *Proceedings of The 11th Annual Network and Distributed System Security Symposium (NDSS '04).* (2004).

[17] Cloudmark Inc. Visited jan 1, 2009. http://www.cloudmark.com/desktop/download/.

[18] Committee on Developments in the Science of Learning and National Research Council. *How People Learn: Bridging Research and Practice*. National Academies Press, 2000.

[19] Cranor, L. F. A framework for reasoning about the human in the loop. In *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security* (Berkeley, CA, USA, 2008), USENIX Association, pp. 1–15.

[20] Danchev, D. Google: Spam volume for q1 back to pre-mccolo levels. CBS Interactive, April 2 2009.

[21] Danchev, D. Microsoft study debunks phishing profitability. ZDNet, January 8 2009.

[22] Dhamija, R., and Tygar, J. D. The battle against phishing: Dynamic Security Skins. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security* (New York, NY, USA, 2005), ACM Press, pp. 77–88.

[23] Dhamija, R., Tygar, J. D., and Hearst, M. Why phishing works. In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems* (New York, NY, USA, 2006), ACM Press, pp. 581–590.

[24] DKIM Signatures, RFC 4871 . Visited jan 1, 2009. http://dkim.org/specs/rfc4871-dkimbase.html.

[25] DOWNS, J., AND FISCHHOFF, B. *Adolescent Health: Understanding and Preventing Risk Behaviors*. John Wiley and Sons, 2009, ch. 5.

[26] DOWNS, J. S., HOLBROOK, M. B., AND CRANOR, L. F. Decision strategies and susceptibility to phishing. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security* (New York, NY, USA, 2006), ACM Press, pp. 79–90.

[27] DOWNS, J. S., HOLBROOK, M. B., AND CRANOR, L. F. Behavioral Response to Phishing. In *eCrime '07: Proceedings of the 2007 e-Crime Researchers summit* (New York, NY, USA, 2007), ACM Press, pp. 79–90.

[28] EBAY INC. Tutorial: Spoof(fake) Emails, 2006. `http://pages.ebay.com/education/spooftutorial/`.

[29] EGELMAN, S., CRANOR, L. F., AND HONG, J. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *CHI '08: Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems* (New York, NY, USA, 2008), ACM, pp. 1065–1074.

[30] EVERETT-CHURCH, R. Mccolo and the difficulty of fighting spam. Internet.com, November 20 2008. `http://itmanagement.earthweb.com/features/print.php/3786296.`.

[31] EVERS, J. Security expert: User education is pointless. CNet News.com, 2006. `http://news.com.com/2100-7350_3-6125213.html`.

[32] FEDERAL TRADE COMMISSION. How Not to Get Hooked by a Phishing Scam, 2006. `http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm`.

[33] FERGUSON, A. J. Fostering E-Mail Security Awareness: The West Point Carronade. EDUCASE Quarterly, 2005. `http://www.educause.edu/ir/library/pdf/eqm0517.pdf`.

[34] FETTE, I., SADEH, N., AND TOMASIC, A. Learning to detect phishing emails. In *WWW '07: Proceedings of the 16th international conference on World Wide Web* (New York, NY, USA, 2007), ACM Press, pp. 649–656.

[35] FINANCIAL SERVICES TECHNOLOGY CONSORTIUM. Understanding and Countering the Phishing Threat. White Paper, 2005. `http://www.fstc.org/projects/docs/FSTC_Counter_Phishing_Project_Whitepaper.pdf`.

[36] FLORENCIO, D., AND HERLEY, C. EVALUATING A TRIAL DEPLOYMENT OF PASSWORD RE-USE FOR PHISHING PREVENTION. In *eCrime '07: Proceedings of the 2007 e-Crime Researchers summit* (New York, NY, USA, 2007), ACM Press, pp. 26–37.

[37] FLYNN, J., SLOVIC, P., AND MERTZ, C. K. Gender, race, and perception of environmental health risks. *Risk Analysis 14*, 6 (1994), 1101–1108.

[38] FRANKLIN, J., PERRIG, A., PAXSON, V., AND SAVAGE, S. An inquiry into the nature and causes of the wealth of internet miscreants. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security* (New York, NY, USA, 2007), ACM, pp. 375–388.

[39] FREE EMAIL PROVIDERS GUIDE. Free email providers list. fepg.net, 2004. `http://www.fepg.net/providers.html`.

[40] FU, A. Y. *WEB IDENTITY SECURITY: ADVANCED PHISHING ATTACKS AND COUNTER MEASURES*. PhD thesis, CITY UNIVERSITY OF HONG KONG, 2007.

[41] GARERA, S., PROVOS, N., CHEW, M., AND RUBIN, A. D. A framework for detection and measurement of phishing attacks. In *WORM '07: Proceedings of the 2007 ACM workshop on Recurring malcode* (New York, NY, USA, 2007), ACM, pp. 1–8.

[42] GARTNER RESEARCH. Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years. Press Release, 2006. `http://www.gartner.com/it/page.jsp?id=498245`.

[43] GARTNER RESEARCH. Gartner survey shows phishing attacks escalated in 2007. Press Release, 2007. `http://www.gartner.com/it/page.jsp?id=565125`.

[44] GEE, J. P. *What Video Games Have to Teach Us About Learning and Literacy*. Palgrave Macmillan, Hampshire, England, 2003.

[45] GOLDMAN, L. Cybercon. Forbes.com, 2004. `http://www.forbes.com/forbes/2004/1004/088.html`.

[46] GOOGLE INC. Google safe browsing for firefox. visited jan 1, 2009, 2007. `http://www.google.com/tools/firefox/safebrowsing/`.

[47] GORDON, L. A., AND LOEB, M. P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur. 5*, 4 (2002), 438–457.

[48] GORLING, S. The myth of user education. In *Proceedings of the 16th Virus Bulletin International Conference* (2006).

[49] GRIMES, R. A. *Malicious Mobile Code: Virus Protection for Windows*, first ed. O'Reilly & Associates, Inc., Sebastopol CA, USA, 2001.

[50] HERLEY, C., AND FLORÊNCIO, D. A profitless endeavor: phishing as tragedy of the commons. In *NSPW '08: Proceedings of the 2008 workshop on New security paradigms* (New York, NY, USA, 2008), ACM, pp. 59–70.

[51] HERZBERG, A., AND GBARA, A. Protecting (even) naive web users, or: preventing spoofing and establishing credentials of web sites. Cryptology ePrint Archive, Report 2004/155, 2004. `http://eprint.iacr.org/2004/155`.

[52] IDENTITY THEFT TECHNOLOGY COUNCIL. Online identity theft: Phishing technology, chokepoints and countermeasures. Report, 2005. http://www.antiphishing.org/Phishing-dhs-report.pdf.

[53] JAGATIC, T. N., JOHNSON, N. A., JAKOBSSON, M., AND MENCZER, F. Social Phishing. *Commun. ACM 50*, 10 (2007), 94–100.

[54] JAKOBSSON, M. The Human Factor in Phishing. http://www.informatics.indiana.edu/markus/papers/aci.pdf, 2006.

[55] JAKOBSSON, M., AND MYERS, S. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Interscience, 2006.

[56] JAKOBSSON, M., AND STAMM, S. Invasive browser sniffing and countermeasures. In *WWW '06: Proceedings of the 15th international conference on World Wide Web* (New York, NY, USA, 2006), ACM Press, pp. 523–532.

[57] JAMES, L. *Phishing Exposed*, 1 edition ed. Syngress, 2005.

[58] JEFF MAKEY. Blacklists compared, april 11, 2009. retrieved april 14, 2009. http://www.sdsc.edu/~jeff/spam/cbc.html.

[59] JOHN E. DUNN. Ie 7.0 tops study of anti-phishing tools , 29 september 2006, techworld. retrieved april 1, 2009. http://www.techworld.com/security/news/index.cfm?newsID=6995&pagtype=sam.

[60] JOHNSON, B. R., AND KOEDINGER, K. R. Comparing instructional strategies for integrating conceptual and procedural knowledge. In *Proceedings of the Annual Meeting [of the] North American Chapter of the International Group for the Psychology of Mathematics Education* (October 2002), vol. 1–4, pp. 969–978.

[61] JUNG, J., AND SIT, E. An empirical study of spam traffic and the use of dns black lists. In *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement* (New York, NY, USA, 2004), ACM, pp. 370–375.

[62] KEIZER, G. Phishers Beat Bank's Two-factor Authentication. Information Week, 2006. http://www.informationweek.com/news/showArticle.jhtml?articleID=190400362.

[63] KJ, P., AND AF., H. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior research methods 40*, 3 (Aug 2008), 879–91.

[64] KLEIN, G. *Sources of power : How people make decisions?* The MIT Press Cambridge, Massachusetts The MIT Press, Cambridge, Massachusetts, London, England, February 1999.

[65] KREBS, B. Host of Internet Spam Groups Is Cut Off. Washington Post, November 12 2008.

[66] KUMARAGURU, P., CRANSHAW, J., ACQUISTI, A., CRANOR, L., HONG, J., BLAIR, M. A., AND PHAM, T. School of phish: a real-word evaluation of anti-phishing training. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security* (New York, NY, USA, 2009), ACM, pp. 1–12.

[67] KUMARAGURU, P., CRANSHAW, J., ACQUISTI, A., CRANOR, L. F., HONG, J., BLAIR, M. A., AND PHAM, T. School of phish: A real-word evaluation of anti-phishing training. In *SOUPS '09: Proceedings of the 5rd symposium on Usable privacy and security* (New York, NY, USA, 2009), ACM.

[68] KUMARAGURU, P., RHEE, Y., ACQUISTI, A., CRANOR, L. F., HONG, J., AND NUNGE, E. Protecting people from phishing: the design and evaluation of an embedded training email system. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems* (New York, NY, USA, 2007), ACM Press, pp. 905–914.

[69] KUMARAGURU, P., RHEE, Y., SHENG, S., HASAN, S., ACQUISTI, A., CRANOR, L. F., AND HONG, J. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *eCrime '07: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (New York, NY, USA, 2007), ACM, pp. 70–81.

[70] KUMARAGURU, P., SHENG, S., ACQUISTI, A., CRANOR, L. F., AND HONG, J. Teaching Johnny not to Fall for Phish. Tech. rep., Carnegie Mellon University, 2006.

[71] KUMARAGURU, P., SHENG, S., ACQUISTI, A., CRANOR, L. F., AND HONG, J. Teaching Johnny not to Fall for Phish. *Transactions on Internet Technology* (2009).

[72] KUNREUTHER, H., AND HEAL, G. Interdependent security. `http://citeseer.ist.psu.edu/kunreuther02interdependent.html`.

[73] LEYDEN, J. Florida man indicted over Katrina phishing scam. The Register, 2006. `http://www.theregister.co.uk/2006/08/18/hurricane_k_phishing_scam/`.

[74] LICHTMAN, D., AND POSNER, E. Holding Internet Service Providers Accountable. CHICAGO JOHN M. OLIN LAW and ECONOMICS WORKING PAPER, 2004. `http://www.law.uchicago.edu/Lawecon/index.html`.

[75] LUDL, C., MCALLISTER, S., KIRDA, E., AND KRUEGEL, C. On the effectiveness of techniques to detect phishing sites. In *DIMVA '07: Proceedings of the 4th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (Berlin, Heidelberg, 2007), Springer-Verlag, pp. 20–39.

[76] MACKINNON, D. P., AND DWYER, J. H. Estimating Mediated Effects in Prevention Studies. *Eval Rev 17*, 2 (1993), 144–158.

[77] MacKinnon, D. P., Fairchild, A. J., and Fritz, M. S. Mediation analysis. *Annual Review of Psychology 58*, 1 (12 2006), 593–614.

[78] Macmillan, N. A., and Creelman, C. D. *Detection Theory: A User's Guide*. Lawrence Erlbaum, 2004.

[79] Maldonado, H., Lee, J.-E. R., Brave, S., Nass, C., Nakajima, H., Yamada, R., Iwamura, K., and Morishima, Y. We learn better together: enhancing elearning with emotional characters. In *CSCL '05: Proceedings of th 2005 conference on Computer support for collaborative learning* (2005), International Society of the Learning Sciences, pp. 408–417.

[80] Mannan, M., and van Oorschot, P. C. On instant messaging worms, analysis and countermeasures. In *WORM '05: Proceedings of the 2005 ACM workshop on Rapid malcode* (New York, NY, USA, 2005), ACM, pp. 2–11.

[81] MarkMonitor. Rock Phishing: Characterization of the Threat and Recommended Countermeasures. whitepaper, 2007. `http://www.markmonitor.com/resources/docs/wp-rockphish-070824.pdf`.

[82] Matthew Broersma. Firefox 2 tops ie 7 in anti-phishing study, 15 november 2006, techworld. retrieved april 1, 2009. `http://www.techworld.com/security/news/index.cfm?newsid=7353`.

[83] Mayer, R. E. *Multimedia Learning*. New York Cambridge University Press, 2001.

[84] Merchant Risk Council. Annual e-commerce fraud survey results. Press Release, March 2009. `https://www.merchantriskcouncil.org/index.cfm?fuseaction=Feature.showFeature&Featur`

[85] Message Anti-Abuse Working Group, and Anti-Phishing Working Group. Anti-Phishing Best Practices for ISPs and Mailbox Providers. Report, 2006. `http://www.apwg.org/reports/bestpracticesforisps.pdf`.

[86] MessageLabs. Messagelabs Intelligence: 2007 Annual Security Report. MessageLabs Intelligence, 2007. `http://www.messagelabs.com/mlireport/MLI_2007_Annual_Security_Report.pdf`.

[87] MessageLabs. Messagelabs Intelligence May 2009. Report, May 2009. `http://www.messagelabs.com/intelligence.aspx`.

[88] Michael Sutton. A tour of the google blacklist, august 7, 2006. visited jan 1, 2009. `http://www.communities.hp.com/securitysoftware/blogs/msutton/archive/2007/01/04/A-T`

[89] Microsoft Corporation. Consumer awareness page on phishing, 2006. Retrieved Sep 10, 2006. `http://www.microsoft.com/athome/security/email/phishing.mspx`.

[90] MICROSOFT CORPORATION. Phishing filter: Help protect yourself from online scams, 2008. http://www.microsoft.com/protect/products/yourself/phishingfilter.mspx.

[91] MILLERSMILES.CO.UK. The web's dedicated anti-phishing service. Retrieved April 15, 2006, http://millersmiles.co.uk/.

[92] MOORE, T., AND CLAYTON, R. Examining the Impact of Website Take-down on Phishing. In *eCrime '07: Proceedings of the 2007 e-Crime Researchers summit* (New York, NY, USA, 2007), ACM Press, pp. 1–13.

[93] MOORE, T., AND CLAYTON, R. The Consequence of Non-Cooperation in the Fight Against Phishing. In *eCrime '08: Proceedings of the 2008 e-Crime Researchers summit* (New York, NY, USA, 2008), ACM Press.

[94] MOORE, T., AND CLAYTON, R. Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing. In *13th International Conference on Financial Cryptography and Data Security* (February 23-26, 2009 2009).

[95] MOORE, T., CLAYTON, R., AND STERN, H. Temporal Correlations between Spam and Phishing Websites. In *2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)* (2009).

[96] MORENO, R., MAYER, R. E., SPIRES, H. A., AND LESTER, J. C. The case for social agency in computer-based teaching: Do students learn more deeply when they interact with animated pedagogical agents? *Cognition and Instruction 19*, 2 (2001), 177–213.

[97] MYSECURECYBERSPACE. Uniform resource locator (URL), 2007. Retrieved Feb 4, 2007, http://www.mysecurecyberspace.com/encyclopedia/index/uniform-resource-locator-url-

[98] NATIONAL CONFERENCE OF STATE LEGISLATURES. 2007 state legislation relating to phishing. Report, 2007. http://www.ncsl.org/programs/lis/phishing07.htm.

[99] NATIONAL CONSUMERS LEAGUE. Avoid getting 'hooked' by phishers, 2006.

[100] NATIONAL CONSUMERS LEAGUE. A Call for Action: Report from National Consumers League Anti-Phishing Retreat. Report, 2006. http://www.nclnet.org/news/2006/Final%20NC%20Phishing%20Report.pdf.

[101] NET APPLICATIONS. INC. . Browser market share q4, 2008. visited jan 1, 2009. http://marketshare.hitslink.com/report.aspx?qprid=0&qpmr=15&qpdt=1&qpct=3&qpcal=1&q

[102] NETCRAFT INC. Netcraft anti-phishing toolbar. visited jan 1, 2009. http://toolbar.netcraft.com/.

[103] NEW MEXICO LEGISLATURE – 2005 SESSION. Sb 720. Law, 2005. http://legis.state.nm.us/Sessions/05%20Regular/final/SB0720.pdf.

[104] NEW YORK STATE OFFICE OF CYBER SECURITY & CRITICAL INFRASTRUCTURE COORDINATION. Gone Phishing: A Briefing on the Anti-Phishing Exercise Initiative for New York State Government. Aggregate Exercise Results for public release, 2005.

[105] OF HOMELAND SECURITY, U. D., COUNCIL, S. I. I. T. T., AND THE ANTI-PHISHING WORKING GROUP. The crimeware landscape:malware, phishing, identity theft and beyond. Report, 2006. http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

[106] ONGUARD ONLINE. Phishing quickfacts, 2008.

[107] PAN, Y., AND DING, X. Anomaly based web phishing page detection. *Computer Security Applications Conference, Annual 0* (2006), 381–392.

[108] PARNO, B., KUO, C., AND PERRIG, A. Phoolproof phishing prevention. In *Proceedings of the 10th International Conference on Financial Cryptography and Data Security (FC'06)* (Feb. 2006).

[109] PENDLETON, B., XIANG, G., AND HONG, J. Augmenting the Crowds: Fighting Phishing on a Budget. Under Submission, 2009.

[110] QUINN, C. N. *Engaging Learning: Designing e-Learning Simulation Games*. Pfeiffer, 2005.

[111] RAMACHANDRAN, A., AND FEAMSTER, N. Understanding the network-level behavior of spammers. In *SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications* (New York, NY, USA, 2006), ACM, pp. 291–302.

[112] REBBAPRAGADA, N. New VoIP Phishing Scams. PCWorld, 2006. http://blogs.pcworld.com/staffblog/archives/001921.html.

[113] REPENNING, A., AND LEWIS, C. Playing a game: The ecology of designing, building and testing games as educational activities. In *ED-Media, World Conference on Educational Multimedia, Hypermedia & Telecommunications* (2005), Association for the Advancement of Computing in Education.

[114] REYNA, V. F., AND FARLEY, F. Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy. *Psychological Science in the Public Interest 7*, 1 (2006), 1–44.

[115] ROSENTHAL, R., AND ROSNOW, R. L. *Essentials of Behavioral Research*, third ed. McGraw Hill, New York, NY, USA, 2008.

[116] ROSS, B., JACKSON, C., MIYAKE, N., BONEH, D., AND MITCHELL, J. C. Stronger password authentication using browser extensions. In *Usenix security* (2005).

[117] ROWE, B. R., AND GALLAHER, M. P. Private sector cyber security investment: An empirical analysis. In *WEIS 2006 - Fifth Workshop on Economics of Information Security* (2006), pp. 18–41. `http://weis2006.econinfosec.org/docs/18.pdf`.

[118] RUSCH, J. J. Phishing and Federal Law Enforcement. Presentation at ABA, 2004. `http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt`.

[119] S. DYNES, H. BRECHBUHL AND M. E. JOHNSON. Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm. In *Fourth Workshop on the Economics of Information Security* (2006), Harvard University.

[120] SALKIND, N. J. *Encyclopedia of Measurement and Statistics*. Sage Publications, 2006.

[121] SCHECHTER, ., DHAMIJA, ., OZMENT, ., AND FISCHER, . The emperor's new security indicators. *sp 00* (2007), 51–65.

[122] SCHNEIDER, F., PROVOS, N., MOLL, R., CHEW, M., AND RAKOWSKI, B. Phishing protection: Design documentation. visited jan 1, 2009. `https://wiki.mozilla.org/Phishing_Protection:_Design_Documentation`.

[123] SCHNEIER, B. Inside risks: semantic network attacks. *Commun. ACM 43*, 12 (2000), 168.

[124] SENDER POLICY FRAMEWORK SPECIFICATIONS (RFC 4408). Visited jan 1, 2009. `http://www.openspf.org/Specifications`.

[125] SHENG, S., HOLBROOK, M., KUMARAGURU, P., CRANOR, L. F., AND DOWNS, J. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Submission: CHI '10: Proceedings of the SIGCHI conference on Human factors in computing systems* (2010).

[126] SHENG, S., KUMARAGURU, P., ACQUISTI, A., CRANOR, L., AND HONG, J. Improving phishing countermeasures: An analysis of expert interviews. In *eCrime Researchers Summit 2009* (Tacoma, WA, USA, 10 2009).

[127] SHENG, S., MAGNIEN, B., KUMARAGURU, P., ACQUISTI, A., CRANOR, L. F., HONG, J., AND NUNGE, E. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security* (New York, NY, USA, 2007), ACM, pp. 88–99.

[128] SHENG, S., WARDMAN, B., WARNER, G., CRANOR, L., HONG, J., AND ZHANG, C. An empirical analysis of phishing blacklists. In *6th Conference in Email and Anti-Spam* (Mountain view, CA, July 16 - 17 2009).

[129] SLOVIC, P. *The Perception of Risk*. The Earthscan Risk in Society Series. Earthscan Publications Ltd, 2000.

[130] State of New York Legislature – 2007 SESSION. A.b 8025. Law, 2007. http://assembly.state.ny.us/leg/?bn=A08025&sh=t.

[131] Symantec. Inc. . Symantec Global Internet Security Threat Report. Tech. rep., Symantec., 2009. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_sec

[132] Thermos, P., and Takanen, A. *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*, first ed. Addison Wesley Professional, 2007.

[133] US House of Representatives. Internet spyware (i-spy) prevention act of 2004. H. R. 4661, 2004. http://thomas.loc.gov/cgi-bin/query/D?c108:5:./temp/~mdbsui94q6::.

[134] US House of Representatives. Internet spyware (i-spy) prevention act of 2005. H. R. 744, 2005. http://thomas.loc.gov/cgi-bin/query/D?c109:11:./temp/~mdbsGYDwP7::.

[135] US House of Representatives. Internet spyware (i-spy) prevention act of 2007. H. R. 1525, 2007. http://thomas.loc.gov/cgi-bin/query/D?c110:7:./temp/~mdbs2yQuGo::.

[136] Varian, H. Managing Online Security Risks, June 2000. New York Times. http://people.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html.

[137] VIRGINIA ACTS OF ASSEMBLY – 2005 SESSION. Chapter 827. Law, 2005. http://leg1.state.va.us/cgi-bin/legp504.exe?051+ful+CHAP0827.

[138] Ward, M. Criminals exploit net phone calls. BBC News, 2006. http://news.bbc.co.uk/2/hi/technology/5187518.stm.

[139] Wu, M. *Fighting Phishing at the Interface Level*. PhD thesis, Massechusets Institute of Technology, 2006. http://groups.csail.mit.edu/uid/projects/phishing/minwu-thesis.pdf.

[140] Wu, M., Miller, R. C., and Garfinkel, S. L. Do security toolbars actually prevent phishing attacks? In *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems* (New York, NY, USA, 2006), ACM Press, pp. 601–610.

[141] Wu, M., Miller, R. C., and Little, G. Web wallet: preventing phishing attacks by revealing user intentions. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security* (New York, NY, USA, 2006), ACM Press, pp. 102–113.

[142] X, S. *Inside the Spam Cartel*, first ed. Syngress Publishing, Inc., Rockland, MA , USA, 2004.

[143] Xiang, G., and Hong, J. An Adaptive Shingling-based Approach using Search Engines for Zero False Positive Phish Detection. Under Submission, 2009.

[144] Xiang, G., and Hong, J. I. A hybrid phish detection approach by identity discovery and keywords retrieval. In *WWW '09: Proceedings of the 18th international conference on World wide web* (New York, NY, USA, 2009), ACM, pp. 571–580.

[145] Ye, Z. E., Smith, S., and Anthony, D. Trusted paths for browsers. *ACM Trans. Inf. Syst. Secur. 8*, 2 (2005), 153–186.

[146] Yee, K.-P., and Sitaker, K. Passpet: convenient password management and phishing protection. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security* (New York, NY, USA, 2006), ACM Press, pp. 32–43.

[147] Zhang, Y., Egelman, S., Cranor, L., and Hong, J. Phinding Phish: An Evaluation of Anti-Phishing Toolbars. In *Proceedings of the ISOC Symposium on Network and Distributed System Security* (2007), Internet Society.

[148] Zhang, Y., Hong, J. I., and Cranor, L. F. Cantina: a content-based approach to detecting phishing web sites. In *WWW '07: Proceedings of the 16th international conference on World Wide Web* (New York, NY, USA, 2007), ACM Press, pp. 639–648.

[149] Zone Alarm. Smart Defense System, 2004. `http://smartdefense.zonealarm.com/tmpl/Advisory`

APPENDIX
Appendix I: List of Recommendations

This section lists the full list of recommendations that I discussed with experts during my interviews.

A.1 Recommendations

This section makes a set of recommendations based on the insights from the phishing analysis (chapter 2) and preliminary stakeholder analysis (chapter 3). The recommendations are categorized into the following framework: prevention, detection, block emails/websites, shutdown, and warn user (see graph 2.9).

The overall objectives are:

1. Catch phishers before they launch attacks

2. Detect attacks as early and accurately as possible

3. Block phishing emails at mail gateways

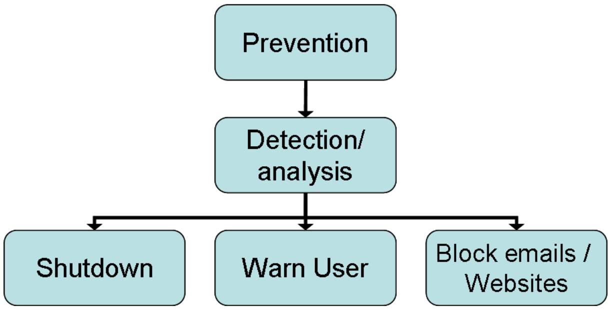

Figure A.1 Taxonomy of phishing technical countermeasures

4. Takedown phishing websites as soon as possible

5. Improve mutual authentication between financial institutions and consumers

6. Minimize money laundering due to phishing

7. Warn and educate users effectively

In the section that follows, I outline recommendations to achieve these objectives.

A.1.1 Prevention

As shown in Figure 2.9, the first step to fight phishing is to prevent attacks before they materialize. Effective law enforcements will reduce the phishers incentive to commit crimes, and will lower the probability of phishers launch attacks after securing personal and corporate resources. Corporate that handle incidents better will be less attractive targets for phishers, and finally proactive measures of anti-phishing from registrars will make setting up phishing attacks much harder. We list the recommendations below.

A.1.1.1 Recommendations for effective law enforcement

1. **Law enforcement: Continue operations to identify and catch phishing gangs such as the Rock Phish gang.** As the underground phishing market improves its efficiency, phishing operations will consolidate and a few organizations will be responsible for most of the phishing. It is estimated that phishing gangs such as Rock Phish are responsible for up to to 50% of phishing. Therefore efforts spent on catching them is necessary. In my interview with law enforcement and other experts, I will consolidate their advice on catching Rock Phish.

2. **Law enforcement, industrial organization, and academia: Provide a more accurate measure of the loss due to phishing in general and particular incident.** There is a lack of data on the monetary losses caused by phishing attacks. It is hard to get for a variety of reasons: banks do not know whether a fraud charge is due to phishing or other activities such as

dumpster driving or malware and the number of people entering information does not mean that the information is correct and can be used by phishers–attacks may not convert to actual losses because banks have sophisticated fraud systems. Confident estimates are important because it is difficult for law enforcement to open cases if they do not have a good idea of the loss. I suggest three possible directions to gather the data: first collect and preserve forensics data when the phishing server is seized, provide a detailed information about the accounts stolen and collaborate with banks to double check these fraud cases; second, study the internet phishing black market for prices of the stolen goods.[1] and lastly, conduct empirical measures, not surveys. Recent efforts by Moore and Clayton [92], Florencio and Herley [36] provide innovative ways to investigate this issue–their methods can be easily shared with law enforcements on a case by case basis to measure the monetary loss both in general and in specific phishing cases.

3. **Regulators: Push the adoption of the cybercrime conventions around the world.** Criminals work their way through the countries that do not comply with the cybercrime convention. To close the loophole, efforts need to be made for countries to ratify the cybercrime convention–a model regulation framework proposed by the European Union.

4. **Law Enforcement: Disrupt the underground black market economy.** As mentioned in Chapter 2.2, phishers, spammers, botnet herders, and pay loaders collaborate to commit crimes and make trades in the Internet black market. Efforts to disrupt the Internet black market will sever the criminals ability to connect with each other. The paper by Perrig and Franklin [38] has outlined a few possible ways to disrupt the market. I recommend further research and action in this area.

   In my expert interviews, I will ask law enforcement experts to comment on these proposals and make suggestions that could enhance phishing law enforcement.

[1] Economics predicts that markets at equilibrium supply equals demand. It is therefore possible to infer the loss due to phishing from the prices of these commodities sold on blackmarkets

A.1.1.2 Recommendations for securing personal and corporate computing resources for anti-phishing

Today, phishing attacks are launched through compromised personal and corporate computers around the world. Spam emails are sent through vulnerable open mail relays and susceptible web forms. Hacked machines host half of the phishing websites. Securing personal and corporate computing environments will make it harder for phishers to launch attacks. Below is a list of security recommendations.

1. **Technology Vendors: Protect host files on user computers.** Some phishing attacks poison DNS records by altering local DNS look up files (except for Windows Vista). Currently, local hosts files are not protected by Windows or by anti-virus software. Protecting these files will help eliminate the DNS poisoning problem and reduce phishing attacks.

2. **Website operators: Check and fix the web form vulnerability for mail injection attacks.** Mail injection attacks can compromise web mail forms, a means for spammers to relay mail. CERT or APWG can also help by producing a toolkit to discover this vulnerability.

3. **Academic institution, CERT, vendors and law enforcement: Continue research and operations to shutdown botnets.** Botnet is the crucial machinery for criminals to launch and evade phishing attacks. Shutting down botnets will not only help eliminate phishing, but a variety of other attacks such as DDOS and spam. However, many have argued that shutting down botnets is not worthwhile for three reasons: vulnerabilities in computers are numerous and it only takes one exploit to control computers; users are careless and are easily fooled into installing malware on their computer; there are hundreds of millions of potentially vulnerable computers connected to the Internet. I think all of these are valid points that acknowledge the difficulty of the task, however, it has been shown in the past that it can be done.

4. **Researchers, Vendors: Research into secure patching for vulnerabilities.** Many computers become infected because of zero day exploits which hackers reverse engineer a patch

and produce exploits and infect computers that are not patched. It can be as little as six hours for an exploit to be created from a patch. Although we would like to see software secure by design, it is unlikely that patches will not be needed. Research into secure patching (possibly using public cryptography) would help alleviate the problem of zero day exploits.

5. **CERT or APWG: Produce a list of most frequently hacked websites and notify the website operators of their vulnerability. Provide toolkits and educational resources to help website operators secure themselves.** Because about 50% of phishing today is on hacked websites[2], this will give incentive for operators to investigate why the websites are hacked and provide them with tools to fix it.

A.1.1.3 Recommendations for improving risk management and incident handling for phishing

1. **Institutions: If frequently targeted, review security procedures and security processes and establish phishing countermeasures.** If a bank is continually being robbed, it means that the security measures in place are inadequate. In the same vein, if phishers continually target an institution, it means that the security measures at the institution need to be improved.

2. **Institutions: Identify a list of high-risk clients and provide education and additional measures to protect them.** Clients such as account executives and business account holders will be at special risk due of phishing because of their networth and their inexperience.

3. **Banking Regulators: Obtain and monitor statistics of the targeted institutions for fraud losses and press the corporations about their security practices if necessary.** As mentioned earlier, there is little data available about fraud losses in banks. Banks do not want to disclose these numbers because they do not have any incentives to do so. Without accurate reporting of these fraud losses, regulators would not know the banks' performance and would find it hard to provide guidance. Requiring banks to report quarterly fraud losses for

[2] According the data we compiled from Phishtank during the two week period in July.

regulator review will help the banks examine their internal processes of control and also help them better manage the process. The data may not need to be public.

A.1.1.4 Recommendations for proactive measures from registrars

1. **Academic Institutions or industry groups: Conduct a study on registrars' preparedness for phishing and other frauds.** Produce best practices for registrars and compile case studies for registrars that prevented phishing.

2. **Regulators (ICANN): Provide guidance and help registrars to detect phishing registrations.** If necessary, issue security standards about phishing for registrars.

A.1.2 Detection

The earlier the detection of attacks, the shorter the response time for shutdown and blocking.

1. **Email Services: Automatically forward suspected phishing emails to antiphishing services at mail gateway level.** Since the email gateway is the first point of contact to phishing emails, phishing emails are freshest here. The difficulty is that mail providers lack incentives to report phishing, because their primary concern is spam. Since most filters do not treat spam and phishing differently, reporting phishing emails at the gateway level means manual work to separate phishing from spam first.

2. **Academic institutions or open source community: Provide a good set of open source phishing filters to integrate with spamassassin.** There are many email providers on the Internet. While large mail providers can deploy sophisticated email filters, smaller and medium size providers usually rely on open source spam filters such as spamassassin. The standard configuration of spam assassin only catches about 70% of phishing emails [34]. To raise the bar for phishing protection, phishers filters should be released to the public domain for free.

A.1.3 Filter email / websites

1. **Encourage mail providers to scan for phishing at mail storage.** In some instances, doing filtering at the mail storage level is preferable–gathering and updating the phishing email signatures take time and some phishing detection techniques require network query (DNS lookup), which would slow down the filter performance dramatically if implemented at gateway (it takes roughly four seconds to process a 10kb email if running network lookup). There is usually a 12-hour lapse between the time mail is in mail storage to the time mail is downloaded to clients computers [100]. Between these stages, some filtering can be applied and mails can be tagged or removed before the client ever downloads them. However, there may be legal and privacy concerns regarding provider examinations of users personal inboxes.

2. **Mail clients could be the next step to combating the problem.** Regular software clients such as Outlook and Thunderbird can run some phishing tests and warn users when the emails are opened. The benefits of doing it here are that there would be no privacy and legal concerns, and mail clients have more information about senders and others for sophisticated filtering.

3. **Web browser vendors: Continue to improve browser anti-phishing toolbar performances, with a goal to catch 85-95% of phishing URLs within an hour.** As shown in Figure 9, Internet Explorer 7 was only able to detect less than 50% of phishing websites within 12 hours, and Safari does not have any phishing protection yet. More efforts here are needed in this area.

4. **Email Providers: Support email authentication SPF and DKIM.** Although email authentication will not solve the problem of email fraud, it does provide accountability in email when used properly. For companies to adopt these methods, email clients must first support them natively.

A.1.4 Shutdown / block phishing websites

1. **CERT or APWG: Produce a list of most frequently hacked websites and constantly monitor websites' security for improvements.** Roughly 50% of phishing is hosted on hacked websites. By producing these statistics, website holders will be aware of their vulnerabilities. Whenever websites are hosted on hacked sites, site owners should be directly notified so that they can take it down and fix its vulnerabilities.

2. **Registrars: Examine solutions to shutdown and suspend Rock Phish domains quickly.**

A.1.5 Warn and educate user

1. **Email clients: Provide effective and integrated warnings for users about phishing messages, and research ways to better present warnings.**

2. **Government, education, and industry groups: Educate consumers about the risks of instant messaging networks.**

A.1.6 Minimize money laundering

The final step is to minimize money loss due to phishing.

To do this, we need to make it harder for third parties to use stolen credentials to commit fraud, and make it more difficult for phishers to launder money even with stolen credentials. My recommendations are:

1. **Financial institutions: Work closely with anti-money laundering communities to ensure that anti-money laundering systems are used to detect phishing related fraud.** Anti-money laundering systems have been used worldwide for many years. To the best of my knowledge, they have not been used to detect phishing fraud. I recommend that phishing rules be added to the AML systems and focus on phishing gangs behaviors. In my expert interviews, I will ask their opinions on these issues.

2. **Regulators (FTC): Launch education campaign to educate the public about mules.** Mules are a crucial element in the underground market, as they transfer money or redirect goods to criminals. Many of the money mules are unaware that the activities they engage in are illegal. As companied with phishing, there are few educational materials in the media about money mules. I recommend regulators such as the FTC organize a campaign against money mules The campaign could either be a standalone campaign or a combined campaign. The format could be testimonials, actual police cases, and recommendations on how not to become a money mule[3].

3. **Industry association: Study money wiring practice of Western Union and Money Gram, especially their security practices about wiring money outside the country.** Western Union and Money Gram are one of the key tools that mules use to transfer money. The system is designed to make money transfer easy, which also makes it easy for criminals. I propose a simple study: to investigate security practice validations and authentications, investigators should visit a dozen local Western Union and Money Gram branches and try to transfer money to Eastern Europe.

A.1.7 Other recommendations

1. **Financial institutions: Implement better mutual authentication systems.** Better mutual authentication means banks can be certain that customers they are dealing with are actually customers, and vise versa. Better-implemented systems will make it difficult for phishers to gain access to accounts even though they may have credential such as usernames and passwords. However, better authentication will not make it impossible to eliminate fraud because we can assume that attackers can gain access to all the credentials that regular customers have (in extreme cases). Although this comes at a higher cost to the attacker, it is not impossible.

2. **Academia** Continue research on mutual authentication.

[3] Recently, Phil H. at Verisign also had the idea of a mule-fool campaign.

3. **Internet service providers: Implement egress and ingress filtering.**

4. **Internet service providers: monitor outbound network traffic from unpatched computers and request users to update.**