

CyberCrime and ID Theft

Be Suspicious

Trust No One
(only slightly kidding)

Chad Crummer
Washington Attorney General's Office



Overview

- **Statistics**
- **CyberCrime Examples We See and Target**
 - Phishing / Smshing
 - 21st Century “Toner Phoner”
 - POS merchants
- **Identity Theft**
 - Tech Protect
 - Physical Protect



Consumer Sentinel Complaints¹

2012 USA Top 10 List

#1 Identity Theft	369,132	18%
#2 Debt Collection	199,721	10%
#3 Banks and Lenders	132,340	6%
#4 Shop-at-Home and Catalog Sales	115,184	6%
#5 Prizes, Sweepstakes and Lotteries	98,479	5%
#6 Impostor Scams	82,896	4%
#7 Internet Services	81,438	4%
#8 Auto Related Complaints	78,062	4%
#9 Telephone and Mobile Services	76,783	4%
#10 Credit Cards	51,550	3%

1) <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf>



2012 Complaints¹

	(Reported)	(Est. Losses)
USA		
Fraud	1,074,937	\$1,491,656,241
ID Theft	369,132	UNKNOWN
WA		(Actual Losses)
Fraud	33,720 (12 th)	\$26,146,146 (14 th)
ID Theft	5,373 (25 th)	UNKNOWN

***Our metro area ranking: 28th highest in the nation for fraud
131st highest for ID theft**

***It is estimated 32% of victims do not contact LE**

1) <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf>



2012 WA FRAUD COMPLAINTS¹

TOP 10 LIST

Fraud and Other Complaints Count from WA Consumers = 33,720

#1 Debt Collection	4,033	12%
#2 Banks and Lenders	2,742	8%
#3 Shop-at-Home and Catalog Sales	2,359	7%
#4 Internet Services	2,178	6%
#5 Impostor Scams	1,944	6%
#6 Telephone and Mobile Services	1,815	5%
#7 Auto Related Complaints	1,540	5%
#8 Prizes, Sweepstakes and Lotteries	1,329	4%
#9 Credit Cards	1,263	4%
#10 Foreign Money Offers/Fake Check Scams	1,098	3%

1) <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf>



2012 WA ID THEFT COMPLAINTS¹

Identity Theft Complaints Count from WA Victims = 5,373

#1 Government Documents/Benefits Fraud	1,268	24%
#2 Credit Card Fraud	1,014	19%
#3 Phone or Utilities Fraud	555	10%
#4 Bank Fraud	541	10%
#5 Employment-Related Fraud	369	7%
#6 Loan Fraud	132	2%
Other	1,412	26%
Attempted Identity Theft	496	9%

1) <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf>



PHISHING / SMSHING

- Scam artists “**phish**” for victims by pretending to be banks, stores, or government agencies. They do this over the phone, in emails, in texts, in postal mail, and sometimes in person attempting to acquire personal information such as passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- **SMShing** is phishing over your cell phone. Scam artists use mobile phone text messages to lure victims into calling back a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.



PHSHING EXAMPLES

TONER PHONER

A business will receive products, often preceded by a phone call, that they never ordered, along with a bill for said product. Sometimes, they don't actually get the products, just a bill. Generally the "products" involved tend to be the ethereal -- like "(phone) line maintenance" or directory listings. Web services are currently in vogue as most of us have no idea what is involved or what we need. We also see real products like janitorial supplies. The scammers' ace in the hole is that many companies don't track what they get, let alone what they order, so the bills just get paid in the normal course of business. The term toner phoner derives from the fact that in years past the primary product involved was copy machine toner.



PHSHING EXAMPLES

Mandatory Posters



THE WASHINGTON LABOR LAW POSTER SERVICE
855 TROSPER ROAD, #108-279
OLYMPIA, WASHINGTON 98512-8108

For compliance assistance
you may call us at: 1-877-321-4144

FAX: 1-888-442-4144

Notice Date: FX-11

Key Code:

**New Washington Minimum Wage
Effective January 1, 2011**

Dear Employer,

State and Federal Law requires Washington employers to post the following notices at most work sites. Investigations may be conducted by State inspectors. An employer found to be in violation of State or Federal Laws by willfully failing to post up-to-date OSHA posters may be subject to monetary penalties of up to \$7000, as well as exposure to civil liability actions. The Washington Labor Law Poster Service is a non-governmental organization providing mandatory workplace posters and does not have a contract with any government agency. Certain posters may also be available free from the issuing governmental agencies. Compliance with State and Federal posting requirements may be achieved by responding to the order form below. **PLEASE RESPOND TODAY TO THE ENCLOSED.**

STATE POSTING REQUIREMENTS

- Notice To Employees**
(Revised Code of WA § 51.14.100)
"Every employer subject to the provisions of this title shall post and keep posted in a conspicuous place or places in an about his place or places of business a reasonable number of typewritten or printed notices of compliance...stating that such employer is subject to the provisions of this title. Such notice shall advise whether the employer is self-insured or has insured with the department...."
- Job Safety and Health Protection**
(Revised Code of WA §49.17.050)
"In the adoption of the rules and regulations under the authority of [the Washington Industrial Safety and Health Act], the director shall: ... provide for the ... posting where appropriate by employers of informational, education, or training materials related to said

FEDERAL POSTING REQUIREMENTS

- Federal Minimum Wage Act (29 CFR § 516.4)**
Pursuant to 29 USC §208(a)(1), as amended by P.L. 110-28, H.R. 2206, effective July 24, 2009, the federal minimum wage increases from \$6.55 an hour to \$7.25 an hour. "Every employer ... shall post and keep posted a notice explaining the Act ... in conspicuous places in every establishment where such employees are employed so as to permit them to observe readily a copy."
- Equal Employment Opportunity is the Law (29 CFR § 1601.30(a) & (b))**
"Every employer ... shall post and keep posted in conspicuous places upon its premises notice in an accessible format ... describing the applicable provisions of title VII and the ADA, and GINA. Such notice must be posted in prominent and accessible places where notices to employees...are customarily maintained...[F]ailure to comply with this section is punishable by a fine of not more than \$110 for each separate offense."
- Family and Medical Leave Act (29 USC §2619)**
"Each employer shall post and keep posted, in conspicuous places on the premises



PHSHING EXAMPLES

Mandatory Posters

and assist in achieving the objectives of this chapter."

- Your Rights as a Worker**
(Washington Administrative Code 296-126-080)
"The employer shall keep posted a current copy of these regulations ... The poster shall be positioned in a readily accessible location and within plain view in each work site where an employee or employees are employed."
- Unemployment Compensation**
(Revised Code of WA § 50.20.140)
"Each employer shall post and maintain printed statements of such rules in places readily accessible to individuals in his or her employment and shall make available to each such individual at the time he or she becomes unemployed, a printed statement of such rules and such notices..."

Also included in our posters:

- * Minimum Wage
- * Discrimination in Employment
- * Discrimination in Places of Public Accommodation
- * Fair Housing

or the employer where notices to employees and applicants for employment are customarily posted, a notice . . . setting forth excerpts from, or summaries of, the pertinent provisions of this subchapter and information pertaining to the filing of a charge."

- Uniform Services Employment and Reemployment Rights Act (38 USCA § 4334(a))**
"Each employer shall provide to persons entitled to rights and benefits under this chapter a notice of the rights, benefits, and obligations of such persons and such employers under this chapter. The requirement for the provision of notice under this section may be met by the posting of the notice where employers place notices for employees."
- Employee Polygraph Protection Act (29 CFR § 801.6)**
"Every employer subject to the EPPA shall post and keep posted on its premises a notice explaining the Act, as prescribed by the Secretary. Such notice must be posted in a prominent and conspicuous place in every establishment of the employer where it can be readily observed by employees and applicants for employment." Under 29 CFR § 801.42(7) a civil penalty not to exceed \$10,000 may be assessed against any employer for violating any provision of this Act.
- Occupational Safety and Health Act (29 CFR § 1903.2(a)(1))**
"Each employer shall post and keep posted a notice or notices ... informing employees of the protections and obligations provided for in the Act ... in a conspicuous place or places where notices to employees are customarily posted. Each employer shall take steps to insure that such notices are not altered, defaced, or covered by other material."

PLEASE MAIL THIS FORM WITH
YOUR CHECK, PAYABLE TO:
**THE WASHINGTON LABOR LAW
POSTER SERVICE**
855 TROSPER ROAD, #108-279
OLYMPIA, WASHINGTON 98512-8108
1-877-321-4144 (phone orders)

Please send the following posters:

Complete Set(s) of Federal and State

___ 1st set..... \$59.50 \$ _____
___ Add'l. set(s)..... \$52.50 \$ _____

Separate Posters

___ Federal Only..... \$24.50 each \$ _____
___ State Set..... \$49.50 each \$ _____

(1st set \$7.75; Shipping \$ _____
add'l sets and Individual
posters \$5.75 each.)..... TOTAL \$ _____

Please Call for Large Order Discounts.

Order Form **FX-11** Key Code:

A complete set is made up of three large posters, one Federal and two State.

Posters are 18" x 24" in full color and laminated in plastic.

Posters also available in Spanish – please call.

PLEASE FAX CREDIT CARD ORDERS TO: 1-888-442-4144 – FAX

Enclosed: Check Money Order Automatic Annual Renewal

Credit Card: VISA MC AmEx Discover

Credit Card #: _____ Exp. _____ / _____

Signature _____

Ship to: (please print clearly) Attention: _____

Company: _____

Address: _____



City: _____ State _____ Zip _____

Phone: (_____) _____



PHSHING EXAMPLES

TONER PHONER




Statement Date	10/26/12
Company Name	[REDACTED]
Account Number	767418246
Amount	\$65.00

221675.60.18425

Contact Us: www [REDACTED]
Questions or Support: info@ [REDACTED]
(360) [REDACTED]
(360) [REDACTED]

[See Account Summary Details](#)

ITEM NO.	DESCRIPTION	AMOUNT
001	Managed DNS Backup Business Services	Annual Fee \$65.00
	• Primary Domain(s) (www.designersedgekitchenandbath.com)	
	• Name Server(s)	
	Name Server 1 (ns37.domaincontrol.com)	Current
	Name Server 2 (ns38.domaincontrol.com)	Current
	Name Server 3 (ns3.dnssvc.com)	Inactive
	Name Server 4 (ns4.dnssvc.com)	Inactive
	• Mail Server(s) (mailstore1.secureserver.net)	Current
002	DNS Failover for 5 A Records	Incl.
003	REST API Access	Incl.
	TOTAL	\$65.00



PHSHING EXAMPLES

TONER PHONER

002	DNS Failover for 5 A Records	Incl.
003	REST API Access	Incl.
		TOTAL \$65.00

- MANAGING AND MAKING CHANGES TO YOUR DNS RECORDS CAN NOW BE DONE AUTOMATICALLY WITH OUR REST API ACCESS SERVICE AVAILABLE AT NO CHARGE FOR ALL ANNUAL SUBSCRIPTION BUSINESS CUSTOMERS. ALL DNS SERVICES INCLUDING SECONDARY EMAIL SERVERS ARE INCLUDED IN YOUR ANNUAL FEE.

- THIS IS A SOLICITATION FOR THE ORDER OF GOODS OR SERVICES, OR BOTH, AND NOT A BILL, INVOICE, OR STATEMENT OF ACCOUNT DUE. YOU ARE UNDER NO OBLIGATION TO MAKE ANY PAYMENTS ON ACCOUNT OF THIS OFFER UNLESS YOU ACCEPT THIS OFFER.

THANK YOU FOR YOUR PAYMENT. WE APPRECIATE YOUR BUSINESS.

Please detach and return this portion with your payment.

Payment Date	Upon Receipt
	767418246
Account Number	
Amount	\$65.00
Enclosed	

Make checks payable to: [REDACTED]
Please include your account number on your check.
DO NOT SEND CASH

Check here and fill out the back of this slip if your billing address has changed or you are adding or changing your email address.

838765 Page 1 of 2



PHISHING EXAMPLES

- Brazen phishers recently even used the FTC and FBI as a cloak. They targeted small and medium-sized companies with bogus complaint files that purportedly originated from government agencies. Once you click on a phishing email, you're typically taken to a phony website that lures victims into giving up their card or bank account numbers. --Bang, the thieves are in.



PHSHING EXAMPLES

Insurance Center (206-237-0734)

People have recently been getting calls on their cell phones from this number. The recording tells the person “your records with the DOL indicate you could be saving money on your car insurance.” and they can press 1 to learn more.

They then collect as much information as possible before the caller eventually has a suspicious light bulb go off.

“Wait, if you have my information from the DOL why do you need my driver’s license number?”



PHSHING EXAMPLES

How's this for a phone call to one consumer on a Sunday night: Visa's fraud unit, calling to ask whether you're aware that \$1,371 has been wired from your bank account via Western Union?

Shockingly this call did not originate from Visa's fraud unit. Visa's fraud unit *doesn't call consumers* when they detect suspicious patterns in such cases. Instead, they call the card's issuing bank, which has the consumer's contact information.

A report from ACI Payment Systems released in October found that **42%** percent of US survey respondents have been victimized by credit, debit or pre-paid card fraud over the prior five years.



PHSHING EXAMPLES

Global Arbitration and Process Servers

Another fake collector trying to cash in on the latest trend in scams. People get calls from a "special investigator" working for Global who proceeds to threaten them with a list of possible actions if they don't settle their past due account. Sometimes people actually owe the debts. Frequently, they not only don't owe the debt, they never did.

In some cases, people actually pay the scammers, often just to be preventative.

Guess who was just added to the sucker list??

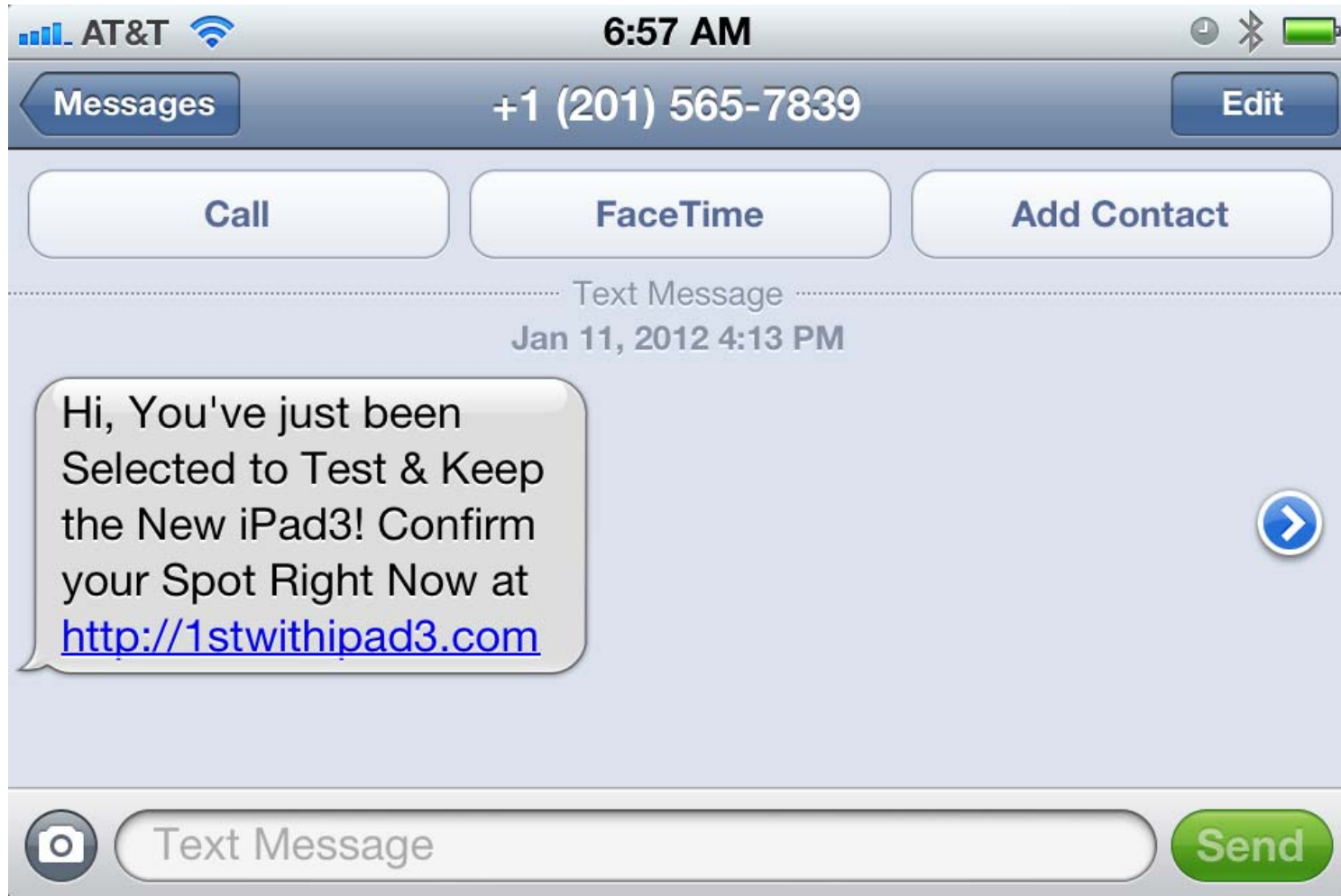


SMISHING EXAMPLES

- You've been randomly selected for a BestBuy gift. Get your \$1,000 gift card at. . .
- WaMu advising the consumer their credit card had been locked down due to possible fraud activity, and a link to the security department to resolve the matter. (this winner didn't realize WaMu no longer existed)



SMSHING EXAMPLES



SMSHING EXAMPLES



RELOADERS

Sucker Lists

Reloaders are crooks who buy lists of people that have fallen for other scams. These lists are uncharitably called "sucker lists." They contact people on those lists by email, mail or telephone with a new scam OR WITH AN OFFER TO RECOVER THEIR LOST cash, baubles, land...

Sadly, reloaders can be as lazy as they want to be. They don't have to speak, understand or even write English well in order to snag victims through a website, email or text.



POS BUSINESSES

Credit Card Machine Leasers and Merchant Processing Services

The merchant is approached by a sales rep and convinced to switch.

Common elements in these situations:

A small business that already has credit/debit processing services, usually through a bank.

A sales representative working for one or another Independent Sales Organization ("ISO") who wants to switch the merchant to their card processing program AND lease them a nice, new terminal.

A bunch of dubious claims about the merchant saving money on transaction fees; and an exorbitant lease on the nice, new card processing terminal that will cost into the thousands of dollars over time even though the terminals can be purchased -- nice and new -- for a mere fraction of that cost.

Often the contract is valid, has lengthy terms, and the cancellation fees can run up to several thousand dollars.



Reduce Your Risk

Identity protection means zealously guarding you and your customer's private information.

- **Make it your first and last thought.**
- **GOOGLE BEFORE DOING ANYTHING!!!**
- **Ask questions.** Whenever you are asked for personal information that seems inappropriate for the transaction, ask questions. Ask how the information will be used, and if it will be shared. Ask how it will be protected. If you're not satisfied with the answers, don't give out personal information.



Reduce Your Risk

- **Treat your trash carefully.** Shred or destroy papers containing personal information including credit card offers and statements. Remember that dumpster-diving is an increasingly lucrative and common occurrence.
- **Protect your postal mail.** Retrieve mail promptly.
- Keep your important papers secure.



Reduce Your Risk

- **Stop pre-approved credit offers.** Pre-approved credit card offers are a target for identity thieves, who steal your mail. Have your name removed from credit bureau marketing lists. You can also call toll-free 888-5OPTOUT (888-567-8688) to do this.



Reduce Your Risk

Tech Protect

- **Protect your computer.** Protect personal information on your computer by following good security practices.
 - Use strong, difficult-to-guess passwords, and check your password strength with a strength checker.
 - Protect your data by using firewall, anti-virus, and anti-spyware software that you update regularly.
 - Download software only from sites you know and trust, and only after reading all the terms and conditions.



Reduce Your Risk

Tech Protect

- **Protect your computer.**

- Don't click on links in pop-up windows or in spam e-mail. Whenever possible YOU should always be the initiator. Stop – Think – Click.
- **Wireless Access Points.** Free public wireless access, for example, in coffee shops or at airports, are ripe for hacker exploitation, because public wi-fi access is the modern equivalent of an old-fashioned telephone party-line.



Reduce Your Risk

Physical Protection

- **Protect your computer.**

- Never leave your computer alone—**even for less than a minute**, without logging out or initiating the password protected screen saver.
- Never leave your computer in a parked vehicle, even if the doors are locked. If you must leave it, hide the computer **and accessories** somewhere in the vehicle, so no one looking in can see any evidence of a computer.



Contact the FTC

- File an identity theft complaint with the FTC:
 - [ftc.gov/complaint](https://www.ftc.gov/complaint)
 - 1-877-ID-THEFT
 - 1-877-438-4338
- Learn more identity theft:
 - [ftc.gov/idtheft](https://www.ftc.gov/idtheft)

