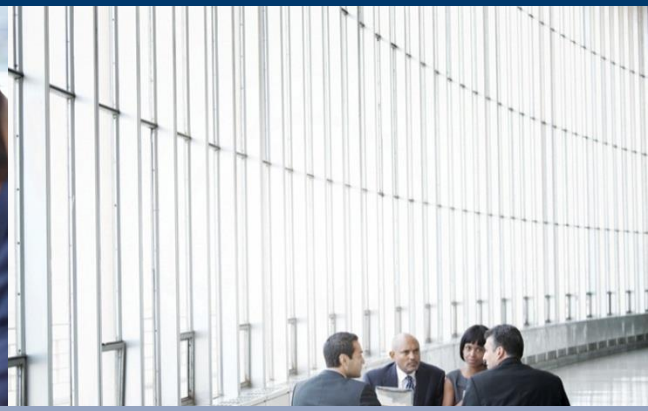




Practical Awareness Program

How we deliver and measure

Eugene Taylashev, Manager

Nellie MacNeil, Sr. Analyst

March 25th, 2015

INTERNATIONAL FINANCIAL DATA SERVICES

Agenda

- About IFDS
- Our challenges and objectives
- Education and Awareness approaches
  - New employee orientation
  - Intranet available policies and procedures
  - Education videos
  - Information Security Calendar
  - Bulletins
  - Phishing simulations
- Measure effectiveness

About IFDS Canada

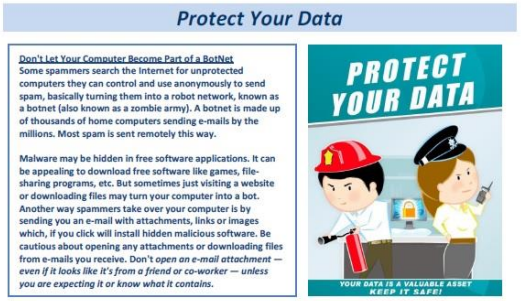
- Premier transfer agency and business process outsourcing solutions provider.
- We are part of the IFDS Group of Companies. IFDS Group has companies in many countries: US, UK, Canada, Ireland, Luxemburg, etc.
- We have our home-built application: Proprietary Transfer Agency system iFAST ™.
- Two 24x7 Data Centers located in Toronto.
- IFDS Canada is ISO 27001 certified.
- The Information Security team has 3 members.
- In scope there are 560 employees and 200 contractors

Our objectives

- Educate employees about cyber security for work and personal life (i.e. Online Safety, Kids and Internet, etc.)
- Train employees and contractors with best user practices (i.e. strong password, clear desk policy)
- Improve protection of customers private and financial data
- Promote our Information Security Management System and Data Leakage Prevention processes
- Remind about importance of Physical Security
- Reduce risk of virus and trojan infections via e-mail phishing
- Address intensive compliancy and audit requirements.

More Education Tools - 1

- Company-specific calendar
  - Contains Information security related mini-articles and pictures
  - All related holidays
  - Company-specific important dates such as “pay days” and “release dates”



Protect Your Data

Don't Let Your Computer Become Part of a BotNet

Some spammers search the Internet for unprotected computers they can control and use anonymously to send spam, basically turning them into a robot network, known as a botnet (also known as a zombie army). A botnet is made up of thousands of home computers sending e-mails by the millions. Most spam is sent remotely this way.

Malware may be hidden in free software applications. It can be appealing to download free software like games, file-sharing programs, etc. But sometimes just visiting a website or downloading files may turn your computer into a bot. Another way spammers take over your computer is by sending you an e-mail with attachments, links or images which, if you click will install hidden malicious software. Be cautious about opening any attachments or downloading files from e-mails you receive. Don't *open an e-mail attachment — even if it looks like it's from a friend or co-worker — unless you are expecting it or know what it contains.*

July 2015

SUN	MON	TUE	WED	THU	FRI	SAT
			1 Canada Day	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17 India End of Ramadan	18
19	20	21 INSTALL TO UAT 15.4	22	23	24	25
26	27	28	29	30 Bangkok Asarnha Bucha Day	31	

August 2015

SUN	MON	TUE	WED	THU	FRI	SAT
						1
2	3 Canada Civic Ireland Bank Holiday	4	5	6	7	8
9	10	11 INSTALL TO UA 15.5 Singapore Queen's Birthday	12 Bangkok Queen's Birthday	13	14	15 Lao Assumption
16	17	18	19	20	21	22
23	24 UK Summer Bank Holiday	25	26	27	28	29
30	31					

Information Security Tip:

- Never reply to SMSs, calls or emails on transactions you did not perform.
- Avoid entering your cell phone number on websites to get free ring tones or other free offers.
- Placing information on a Cloud or Dropbox leaves it vulnerable to be misused by others.

International Financial Data Services

Information Security Bulletin

The Information Security Team :
Nellie MacNeil – ext. 5222
Felix Shin – ext. 5484
Eugene Taylashev – ext. 5060
Kevin Luong –ext. 5658

March 2015

What is Malvertising?

What is it?

Malvertising is the name the security industry gives to criminally-controlled advertisements which intentionally infect people and businesses. These can be any ad on any site – often ones which you use as part of your everyday Internet usage. While the technology being used in the background is very advanced, the way it presents to the person being infected is simple. To all intents and purposes, the ad looks the same as any other, but it has been placed by a criminal.

Without your knowledge, a tiny piece of code hidden deep in the ad is making your computer go to criminal servers. These then catalogue details about your computer and its location, and then choose which piece of malware to send you. This doesn't need a new browser window and you won't know about it.

The first sign will often be when the malware is already installed and starts logging your bank details or any number of despicable scams.

How do they get there?

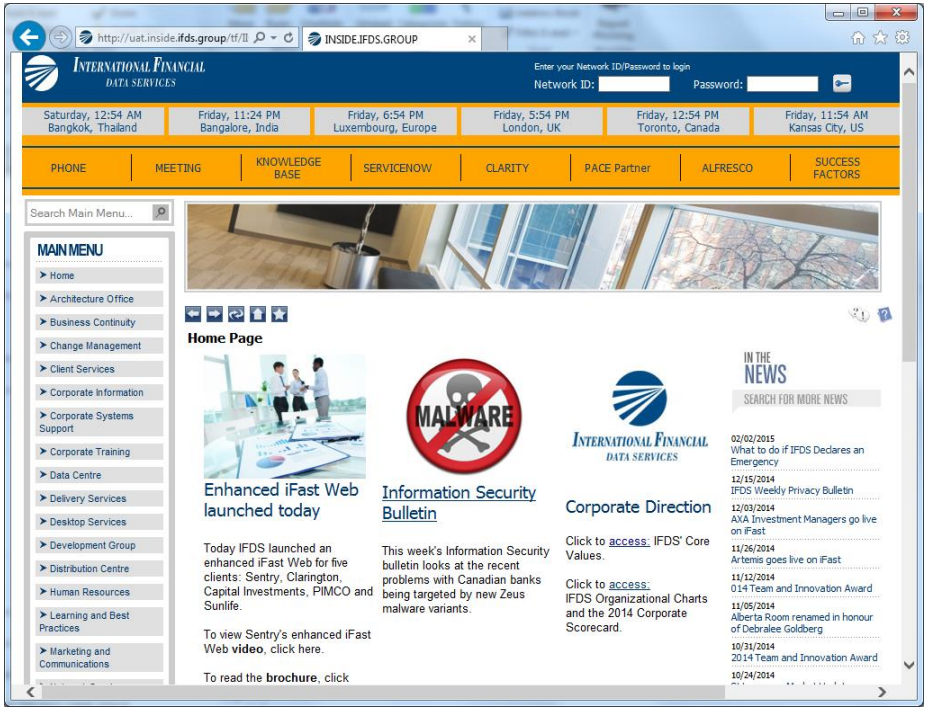
It's common practice to outsource the advertising on websites to third-party specialists. These companies re-sell this space, and provide software which allows people to upload their own ads, bidding a certain amount of money to 'win' the right for more people to see them.

This often provides a weak point, and cyber criminals have numerous clever ways of inserting their own malicious ads into this self-service platform. Once loaded, all they have to do is set a price per ad, to compete

Monthly bulletins with Information Security trends updates. Placed in common access places.

More education tools - 2

- Comprehensive Acceptable Usage Policy (AUP), attested to annually.
- Surprise Clear Desk inspections.
- Policies and procedures found online in the Intranet.
- Online Learning Management System (LMS) is also used.



Annual Awareness Week

- A 20 minute education video session with quiz, small give-away and treats.
- Annual event. We provide 20 sessions during a week in May, and then few additional sessions for people who missed.
- Mandatory for all employees and contractors.
- Quality of understanding is verified by a quiz at the end.

Our Simulated Phishing Program

Background:

After seeing more and more phishing emails passed through the email security system and falling victims with low awareness, IFDS decided to introduce simulated phishing program in 2014.

This monthly program consists of:

- Draft email with the content similar to recent phishing trends.
- Send email and track the activities from the recipients.
- Provide education after each simulation.


Hey [redacted] check this out LOL!

You gotta see the other pictures that are attached -- hilarious!!

-Sandy

Begin forwarded message:

LOL those are great! Thanks Gary!

To: Clare Mclain <cmclain@clarkington.edu>
From: James Conyers <james.conyers@vandelayind.com>
Subject: check this out!

Check out these kitties! :-)

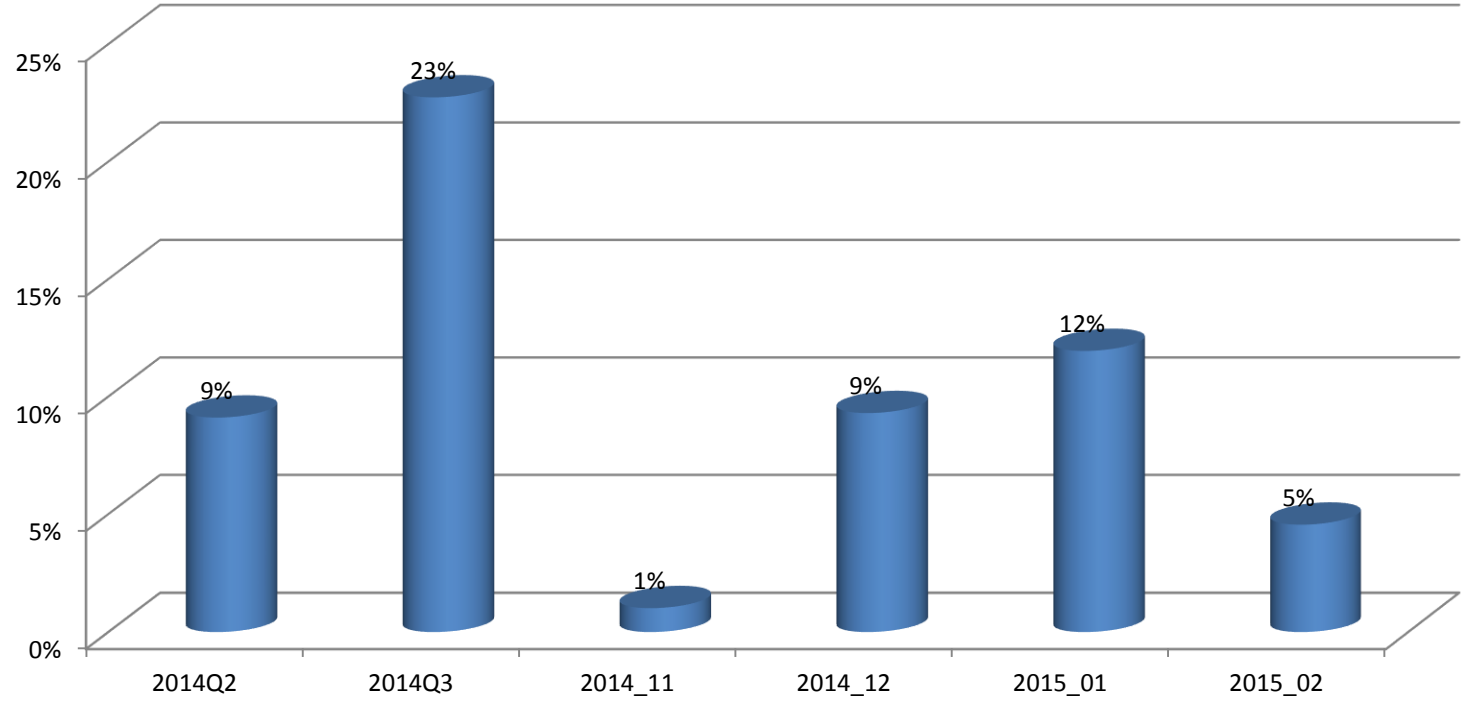
Gary

Clare Mclain
Office of Student Affairs
Clarkington University

Simulated Phishing Program - Stats

Result:

The result is mostly based on how the email content is convincing and related to the company.



Simulated Phishing Program - Results

What we learned:

- The program is a continual process. Stay away from the mindset – we deploy and we forget.
- Use a similar email content or scenario at least 5 times – it will bring up the awareness and stick with the employees longer.
- Tackle the repeated offenders – find out why they keep failing and provide specific training content.
- Encourage the employees to report – the more samples you have, the better security controls can be placed to prevent.
- Think of the employees as the last and valuable phishing detection sensors – better trained employees will detect more without falling into phishing.

Effectiveness Measurements

- Ratio of planned Awareness Training campaigns - 100%
- Ratio of employees and contractors that have completed security training and have been tested – 98.49%
- Dollars spent on awareness per person:
  - 2014, no phishing - $6.58 CAD
  - With phishing (estimate) - $25 CAD

- Simulated Phishing results

	Our rate	Other customers (aver)	Financial Industry
2014 Q2	9%	n/a	n/a
2014 Q3	23%	n/a	n/a
2014 Nov	1%	n/a	n/a
2014 Dec	9%	20%	21%
2015 Jan	12%	17%	12%
2015 Feb	5%	22%	14%

- Repeated phishing offenders:
  - >3 times repeated: None
  - 3 times repeated: 3
  - 2 times repeated: 24

Eugene Taylashev

Nellie MacNeil

Practical Awareness Program