

Economics of Information Security

Thursday, October 21, 2010
CS342 Wellesley
Tyler Moore

Why Economics?

- Economics: “the study of how society uses its scarce resources” ([The Economist](#))
- Conventional threat modeling has failed
 - Enumerate possible threats
 - Define attacker capabilities
 - Build systems to protect against these threats
 - Worked for encryption algorithms, but not Internet security
- Attackers operate *strategically*
 - Must understand what motivates attackers
 - Cannot expect attackers to respect stated assumptions of behavior




Why Economics?

- Many good security schemes aren't adopted
 - Verizon-Secret Service study: 64% of breaches could have been prevented using “simple and cheap” countermeasures
(Source: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xq.pdf)
 - Security failure cannot be explained by lack of technical innovation
- Defenders also operate *strategically*
 - Must understand incentives of defender

Outline of topics covered

- Incentives of attackers and defenders
- Economics of IT vs. traditional industries
- Key market failures
 - Information asymmetries
 - Externalities
- Next week
 - Econometrics: measuring attack and defense
 - Policy interventions available

The power of incentives

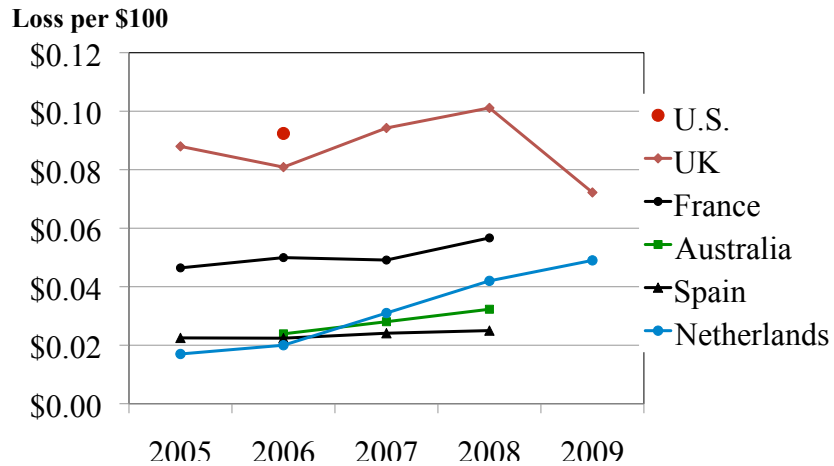
- Systems often fail because people who could protect a system have no incentive to do so
- Re  nking security in the 1990s
 -  US banks must pay for ATM card fraud
 -  In UK, regulators favored banks, often made customer pay for fraud



UK card holders experience more fraud

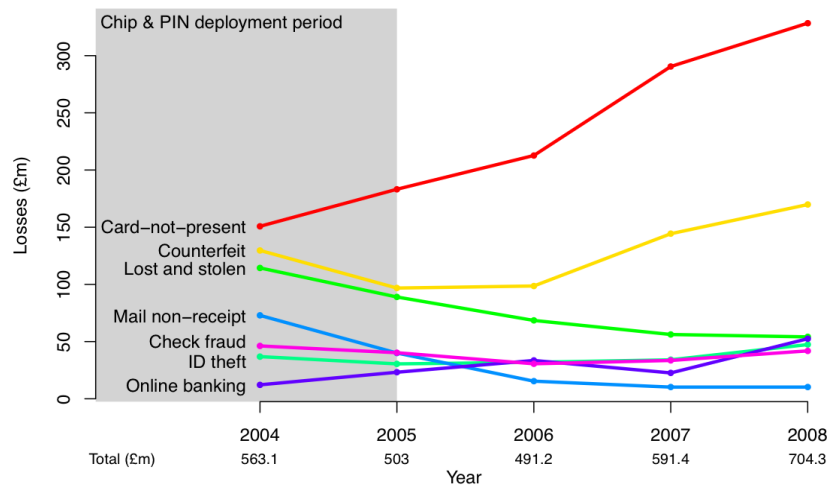
- In the US, because disputed transactions must be paid for by banks, the banks had a strong incentive to invest in technology to reduce fraud
- In the UK, because banks could blame customers, they did not have a strong incentive to invest in the same anti-fraud mechanisms
- Fraud levels grew higher in the UK over time, and remain substantially higher to this day

Comparing card fraud across countries



R. Sullivan, http://weis2010.econinfosec.org/papers/panel/weis2010_sullivan.pdf

Attacker adaptation in UK payment card fraud



S. Murdoch, S. Drimer, R. Anderson, Chip and PIN is broken. <http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf>

Monday, October 18, 2010 New York 69°/49°

THE WALL STREET JOURNAL | TECH

U.S. Edition Home Today's Paper Video Blogs Journal Community Log In

World U.S. New York Business Markets Tech Personal Finance Life & Culture Opinion Careers Real Estate Small Business

Digits Personal Technology What They Know All Things Digital

TOP STORIES IN Technology

1 of 12 Chief Defends Yahoo Amid Slack Sales

2 of 12 Apple Updates MacBook Air

3 of 12 Galaxy Tab to Cost \$600

New York Microsoft

WHAT THEY KNOW | OCTOBER 18, 2010

Facebook in Privacy Breach

Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds

Article Video Comments (161) MORE IN TECH

Email Print Save This Like 72K + More Text

By EMILY STEEL And GEOFFREY A. FOWLER



Kim White Bloomberg

Facebook founder and CEO Mark Zuckerberg addressed the F8 developer conference this spring.

Many of the most popular applications, or "apps," on the social-networking site Facebook Inc. have been transmitting identifying information—in effect, providing access to people's names and, in some cases, their friends' names—to dozens of advertising and Internet tracking companies, a Wall Street Journal investigation has found.

More From What They Know

- Facebook in Privacy Breach
- 'Scrapers' Dig Deep for Data on Web
- Kids Face Intensive Tracking on Web

About This Project

Marketers are spying on internet users - observing and remembering people's clicks, and building and selling detailed dossiers of their activities and interests. The Wall Street Journal's What They Know series documents the new, cutting-edge uses of this internet-tracking technology and the implications for consumers.

Latest Tweets Follow

Congressmen Send Letter to Facebook About Privacy Breach <http://bit.ly/9SYUWm>
6 hrs 5 min ago from WhatTheyKnow (WSJ's What They Know)

RT @ralco RT @normative: Most disturbing aspects of the

← → C online.wsj.com/article/SB10001424052748704513104575256701215465596.html

THE WALL STREET JOURNAL Digital Network WSJ.com MarketWatch BARRONS All Things Digital. FINIS StartMoney More News, Quotes, Companies, Videos SEARCH

Friday, May 21, 2010 New York 62°/43°

THE WALL STREET JOURNAL | TECH

U.S. Edition Home Today's Paper Video Blogs Journal Community Log In

World U.S. New York Business Markets Tech Personal Finance Life & Culture Opinion Careers Real Estate Small Business

Digits Personal Technology What They Know All Things Digital

TOP STORIES IN Technology

1 of 12 Microsoft's New Windows Phone 7

2 of 12 Apple Updates MacBook Air

3 of 12 PayPal Lifts EBay Profit

TECHNOLOGY | MAY 21, 2010

Facebook, MySpace Confront Privacy Loophole

Article Video Stock Quotes Comments (37) MORE IN TECH

Email Print Save This Like 6K + More Text

By EMILY STEEL And JESSICA E. VASCELLARO

Facebook, MySpace and several other social-networking sites have been sending data to advertising companies that could be used to find consumers' names and other personal details, despite promises they don't share such information without consent.

Journal Community

- Vote: How would you grade Facebook's handling of users' privacy?

Related

- Full Text: On the Leakage of Personally Identifiable Information Via Online Social Networks

The practice, which most of the companies defended, sends user names or ID numbers tied to personal profiles being viewed when users click on ads. After questions were raised by The Wall Street Journal, Facebook and MySpace moved to make changes. By Thursday morning Facebook had rewritten some of the offending computer code.

Advertising companies are receiving information that could be used to look up individual profiles, which, depending on the site and the information a user has made public, include such things as a person's real name, age,

Most Popular in Tech

- Verizon to Offer Cheaper Data Plan
- Facebook in Privacy Breach
- More Questions for Facebook
- Tech Rivals Wage War of Words
- Parents Use iPad for Speech Therapy

Most Popular on Facebook

- Karl Rove: Obama's Incoherent Closing Argument - WSJ.com 484 people shared this.
- Facebook in Online Privacy Breach; Applications Transmitting Identifying Information - WSJ.com 72,766 people shared this.
- Geithner's Goal: Rebalanced World Economy - WSJ.com 293 people shared this.

How history repeats itself

- May 2010 privacy leak (benedelman.org)

<http://www.facebook.com/bedelman?ref=profile#!/pacoles>

```
GET /deals/socialads_reflector?do_not_redirect=1&preferred_city=152&ref=AUTO_LOWE_Deals_1273608790_uniq_bt1_b100_oci123_gh_a21-99 HTTP/1.1
Accept: */*
Referer: http://www.facebook.com/bedelman?ref=profile
...
Host: livingsocial.com
...
```

- October 2010 privacy leak (freedom-to-tinker.com)

[http://fb-tc-2.farmville.com/flash.php?...fb_sig_user=\[User's Facebook ID\]...](http://fb-tc-2.farmville.com/flash.php?...fb_sig_user=[User's Facebook ID]...)

- Facebook may take a PR hit for this, but otherwise stands little to lose

Incentives and privacy breaches

- Recall: 64% of privacy breaches could have been prevented using “simple and cheap” countermeasures
- Who suffers when a firm loses personal information?
 - The subjects whose information is revealed
 - The managing firm’s only costs are usually reputational
 - Why spend lots of money, even on “simple and cheap” countermeasures, when the cost of failure is low and uncertain?

IT Economics

- Economic 'rules' for the IT industry differ from those for other industries
- Rule #1: Network effects
 - Value of a network grows super-linearly to its size

- Fax
 - ...
 - n^2
- operating system or n log



– Upshot: hard to bootstrap success, hard for

home | reviews | **news** | downloads | video

cnet news

Latest News | CNET River | Webware | Crave | Business Tech | Green Tech | Wireless | Security | Blogs

Home > News > News Blog

News Blog

Recent posts on technology, trends, and more

February 24, 2008 12:17 PM PST

YouTube blames Pakistan network for 2-hour outage

by Greg Sandoval

Font size | Print | E-mail | Share | 3 comments

[Tweet](#) [Share](#)

Updated, 9:40 p.m. to add YouTube's explanation of what caused outage.

YouTube suffered a two-hour long, system-wide outage on Sunday that the company said was triggered by a network based in Pakistan.

YouTube
Broadcast Yourself

"For about two hours, traffic to YouTube was routed according to erroneous Internet Protocols," said YouTube spokesperson Ricardo Reyes in a statement "Many users around the world could not access our site. We have determined that the source of these events was a network in Pakistan. We are investigating and working with others in the Internet community to prevent this from happening again."

The **BBC reported** that Pakistan's attempts to block access to YouTube may have inadvertently caused the outage. Earlier in the day, Pakistan's shutoff access to YouTube inside the country in response to the posting of cartoons of the Prophet Mohammad, which have outraged many Muslims.

Most Popular

- Has Facebook lost control of the F...
- Help! My PC is infected with malw...
- Laptop thief backs up victim's dat...
- A misguided rebuttal to Steve Job...
- Apple gets 'Back to the Mac' with i...
- Lion (live blog)

CNET River

- A look inside the new M...**
- Star Wars: The Force Un...**
- Ep. 1333: Introducing the**

Network Effects and Infosec

- Many technical security solutions become effective only when many people adopt them
 - Introduced in 1996, S-BGP authenticates the paths routers advertise and could have prevented Pakistan telecom from shutting down YouTube
 - However, S-BGP is only valuable if all ISPs switch
 - Why is email still sent unauthenticated?
- Security protocols which have succeeded offer immediate value to adopting firms

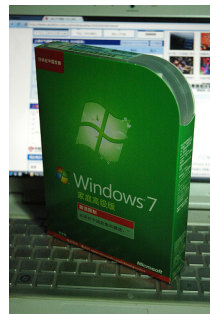
IT Rule #2: High fixed costs and low marginal costs of production

Traditional industry: high fixed & high marginal costs



CC licence: Flickr user CanadaGood

IT industry: high fixed & low marginal costs



CC licence: Flickr user Richard Bao

Competition drives price down to marginal costs of production (i.e., \$0!)

IT Rule #3:

Switching costs determine value

- Switching from one IT product or service is usually expensive
- Shapiro-Varian theorem
 - net present value of a software company is the total switching costs
 - Once you have \$1000 worth of songs on your iPod, you're locked into iPods
 - Why can Microsoft still charge for Office despite 'free' alternatives?
- Beware security mechanisms used to promote lock-in (e.g., digital rights management)

IT Economics and Security

- The high fixed/low marginal costs, network effects & switching costs in information industries all tend to lead to dominant-firm markets with big first-mover advantage
- So time-to-market is critical
- Microsoft philosophy of 'we'll ship it Tuesday and get it right by version 3' is not perverse behavior by Bill Gates but quite rational
- Whichever company had won in the PC OS business would have done the same

When markets fail



http://en.wikipedia.org/wiki/Flash_crash

When markets fail

- Market failures occur when the free-market outcome is inefficient
 - Monopolies/oligopolies
 - Public goods
 - Information asymmetries
 - Externalities
- Market failures justify regulatory intervention, and inform how public policy should be designed
 - They help explain why private information security investment is often suboptimal

Markets with asymmetric information



CC Flickr
user:
Matt Niemi

Akerlof's market for lemons

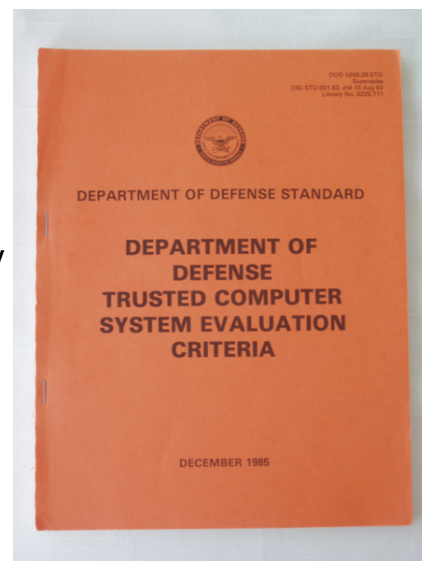
- Suppose a town has 20 similar used cars for sale
 - 10 'cherries' valued at \$2,000 each
 - 10 'lemons' valued at \$1,000 each
 - What is the market-clearing price?
- Answer: \$1,000. Why?
 - Buyers cannot determine car quality, so they refuse to pay a premium for a high-quality car
 - Sellers know this, and only owners of lemons will sell for \$1,000
 - The market is flooded with lemons

Secure software is a market for lemons

- Vendors may believe their software is secure, but buyers have no reason to believe them
- So buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to do so
- How might the information asymmetry be reduced?
 - Option 1: certification schemes
 - Option 2: collect better data

Option 1: certification schemes

- Common Criteria certification
 - Sometimes useful, but may be gamed
 - Evaluation is paid for by vendor seeking approval, leading to




Google mbt kaya Search

About 406,000 results (0.32 seconds) Advanced search

Everything
 Images
 Videos
 Shopping
 More

All results
 Fewer shopping sites
 More shopping sites
 More search tools

Shopping results for mbt kaya

 [MBT Kaya - MBT Women's Maryjane Shoes](#)
 \$127.48 new - Zappos.com
[MBT Kaya - MBT Women's Maryjane Shoes](#)
 \$127.48 new - 6pm
[MBT Kaya - Black](#)
 \$119.95 new - ShoeStores.com

MBT Kaya Shoes, MBT Kaya Sale, MBT trainers ☆ - Oct 19
 Discover the benefits of **MBT Kaya**. We supply best quality of **MBT Kaya** shoes, more discount mbt shoes on mbtshoestar.com. Fast delivery, highest quality, ...
www.mbtshoestar.com/mbt-kaya-shoes-c-83.html - Cached

Amazon.com: MBT Women's Kaya Mary Jane: Sports & Outdoors: Reviews... ☆
 Footwear with a unique sole construction that mimics the feeling of walking barefoot on sand, activating muscles throughout the body and relieving stress on ...
www.amazon.com > ... > Women's > Fashion Sneakers > Mary Janes - Cached

Mbt Kaya on Footwear etc. ☆
 Read 91 Reviews for **MBT Shoes: MBT Women's Kaya Mary-Jane - Chocolate Nubuck - On Sale!** Related Searches: **Mbt Sale | Mbt | Kaya** ...
shoes.footwaretc.com/footwear/Mbt%20Kaya - Cached - Similar

MBT Kaya Chocolate - Zappos.com Free Shipping BOTH Ways ☆
 Kaya by MBT at Zappos.com - FREE Shipping. Read **MBT Kaya** product reviews, or select the **MBT Kaya** size, width, and color of the **MBT Kaya** of your choice.
www.zappos.com/mbt-kaya-chocolate - Cached - Add to iGoogle


MBT Kaya | cheap MBT Kaya. mbt sport sale.com ☆
 cheap **MBT Kaya** -mbt shoes, mbt sport shoes for sale, A lot of **MBT Kaya** for you to choose in our mbt sport sale.com store. **MBT Kaya** good to care your body.
www.mbt sport-sale.com/mbt-kaya-c-9.html - Cached

Not all shoe websites are created equal

zappos.com



mbt sport-sale.com

SHOP WITH CONFIDENCE

 SHOPPING ON ZAPPOS.COM IS SAFE AND SECURE. GUARANTEED!

You'll pay nothing if unauthorized charges are made to your credit card as a result of shopping at Zappos.com.

SAFE SHOPPING GUARANTEE

All information is encrypted and transmitted without risk using a Secure Sockets Layer (SSL) protocol.
[Learn How We Protect Your Personal Data >](#)










Copyright © 2010 mbt sport sale. Powered by Sale Online Store

```

Domain Name ..... mbt sport-sale.com
Name Server ..... dns15.hichina.com
                  dns16.hichina.com
Registrant ID ..... hc504175808-cn
Registrant Name ..... Joe Susan
Registrant Organization ..... Organization CXGroup
Registrant Address ..... no.25 lvring road,siming district.
Registrant City ..... xiamen
Registrant Province/State ..... Fujian
Registrant Postal Code ..... 361009
Registrant Country Code ..... CN
Registrant Phone Number ..... +86.592519411 - 0
Registrant Fax ..... +86.592519411 - 0
Registrant Email ..... micheltalor@gmail.com
    
```



Adverse selection in certification schemes

- Edelman uses data from SiteAdvisor to identify sites distributing spam and malware as 'bad'
 - He then found that such 'bad' companies are more likely to be TrustE-certified: 5.4% of TrustE-certified sites are 'bad', compared with 2.5% of all sites.
 - Similarly, untrustworthy sites are over-represented in paid advertisement links compared to organic search results
- This is called *adverse selection*
 - In health insurance, adverse selection occurs when sick people are more likely to buy coverage than healthy people
 - Consequence of markets with asymmetric information

Moral hazard

- The second classical outcome of asymmetric information is moral hazard
 - People may drive recklessly if fully insured with \$0 deductible
- Moral hazard in information security
 - Often claimed that consumers engage in moral hazard due to \$0 card fraud liability
 - Cuts both ways: when regulations favor banks, they can behave recklessly in combating fraud

Option 2: Collect information to measure security

- Auto insurance companies could offer lower premiums to people who install speed-monitoring devices
 - Similarly, measures of information security could be collected to differentiate safe vs. unsafe websites, secure vs. insecure software, etc.
 - More on this next week

Externalities



http://en.wikipedia.org/wiki/File:Zona_Leste_-_S%C3%A3o_Paulo-Brasil.jpg

Externalities

- Cost (or benefit) incurred by a party who did not agree to the transaction causing harm (or benefit)
 - Positive externalities tend toward under-provision
 - Negative externalities tend toward over-provision
- Environmental pollution is a negative externality
 - Factory produces a good and gets paid by buyer
 - Pollution caused by production is not accounted for in the transaction
- Information insecurity is a negative externality

Botnets



Source: <http://en.wikipedia.org/wiki/File:Botnet.svg>

Botnet infections as an externality

- Botnets carry out the task requested by botnet herder
 - Send spam
 - Host phishing websites
 - Distribute malware
 - Launch denial-of-service attacks
- Many tasks assigned to bots are designed to harm others more than their host

Cyber attacks in Estonia April 2007



Incentives of botnet participants

- Botnet operators (\$)
- End users
 - Many are unaware of compromise, and the malware is designed to harm others
- ISPs
 - Often aware of customers that are infected
 - If too much spam is sent, then other ISPs may blacklist them
 - Quarantining customers is expensive (in terms of kit and especially calls to customer support)

Other examples of insecurity externalities

- Industrial control systems
 - Critical infrastructure operators have moved connected their control systems to IP networks to reduce near-term cost
 - Increased risk of an outage is discounted because costs are borne by society
- If persistent insecurity keeps people from using the Internet, then positive externalities of Internet usage go squandered

Summary of today's lecture

- Incentives explain security investment
- Economics of IT industries tend toward dominant firms
- Information security is frequently characterized by 2 market failures
 - Information asymmetries
 - Externalities
- To really improve security, we must work to correct these failures

Looking ahead to next week

- Measuring Internet crime
 - Phishing
 - Botnets
- Improving information security through policy
 - Information disclosure
 - Intermediary liability

Project ideas

- Tracking online censorship on Herdict
 - Improving the crowd's assessment of blockage
 - Reputation of reporters
 - Comparing Herdict reports to news and twitter reports
- Tracking High Yield Investment Program scams
- Tracking fake shoe shops
- Analyzing privacy breach reports on datalossdb.org

ENGLISH | العربية | 中文 | हिन्दी | РУССКИЙ

BETA
HERDICTWEB
THE VERDICT OF THE HERD

EXPLORE PARTICIPATE ABOUT HOME

FIND A REPORT
Choose a country

ADD AN ALERT Want to know when your favorite site is inaccessible? Sign up for e-mail alerts [here](#).

PARTICIPATE What's your verdict? Participate in Herdict Web today.

www.youtube.com in All Countries All time

www.youtube.com was reported **inaccessible 3,922** times around the world.
www.youtube.com was reported **accessible 4,205** times around the world.
This site ranks **1** out of **4,684** reported sites.

Reports

URL	DATE	REPORTS	ISP	COUNTRY	COMMENTS
▼ YouTube - Broadcast Yourself. (176 / 324)					
www.youtube.com	2007-05-31 00:00:00.0	×	KACST	Saudi Arabia	ONI survey 2007
www.youtube.com	2009-01-23 16:47:40.0	✓	EBNE-YAMIN POP SITE	Iran	
www.youtube.com	2009-01-28 12:09:39.0	×	SCS-NET IS AN ISP BASED IN DAMASCUS SYRIA	Syria	
www.youtube.com	2009-01-28 15:22:31.0	✓	HARVARD UNIVERSITY	United States	
www.youtube.com	2009-01-28 16:48:03.0	✓	HARVARD UNIVERSITY	United States	
www.youtube.com	2009-01-28 18:50:28.0	✓	HARVARD UNIVERSITY	United States	
www.youtube.com	2009-01-28 19:57:48.0	✓	TISCALI UK LTD	United Kingdom	
www.youtube.com	2009-01-28 22:03:59.0	✓	KOREA TELECOM	South Korea	
www.youtube.com	2009-01-29 12:08:13.0	✓	ADN	Austria	
www.youtube.com	2009-01-29 13:26:01.0	✓	HARVARD UNIVERSITY	United States	
www.youtube.com	2009-01-29 15:09:06.0	✓	HARVARD UNIVERSITY	United States	
www.youtube.com	2009-02-09 15:05:03.0	✓	REASSIGN TO SUKHUMVIT REALSTATE CO. LTD	Thailand	
www.youtube.com	2009-02-10 14:23:06.0	×	BRIGHAM YOUNG UNIVERSITY	United States	The school blocks YouTube, unless you are a professor who needs it for class.

money princ. in daily rock payments, robust and secure for our investors.

Your site here for \$260

FINANCES ADVISOR
This is the place where you can earn a lot of money with or without any referrals. You do not have to recruit anyone, neither meet anyone. You don't have to carry any stock or be constantly traveling.

Your site here for \$240

CHERRYSHARES
Cherryshares is Brooksell Universal Limited Company. The arena of private investing has always been the area of the extremely rich. A few years ago, our private investment pool has the doors opened to a select few people to invest.

Your site here for \$250

FOREX COMPANY ONLINE
International market FOREX (FOREIGN EXCHANGE MARKET) is currently the main source of income for many banks, companies, some enterprises and even experienced private traders working independently.

Your site here for \$240

Your site here for \$240

Your site here for \$230

+ Add site All Premium

LINK TO US >>

HYIP News:

19.10 News of Umsamo Fund
Affiliate Program Update
We have received numerous e-mails from our customers who have asked us to expand our affiliate program. We decided to use an experimental, a little more complicated system of our affiliate program for a period of

SMARTER PROFITS - COMPUTERIZED LOGISTICS™

Premium Ads on HYIP.COM / Your ad here for only \$ 250 / week across HYIP.com: [Bid now >](#)

CherryShares	Status: PAYING Our Investment: \$1210 Min/Max: \$50 Referral: 3.00% - 25.00%	Monitored: 533 days Profit: 0.83% - 1.41% daily Period: up to 525 days Withdrawal: Instant	User Rating: ☆☆☆☆☆ (1494 users) Our Rating: ☆☆☆☆☆ ROI: 149% PROFITABLE HYIPRANK: 1 / 1856
Cherryshares is Brooksell Universal Limited Company. The arena of private investing has always been the area of the extremely rich. A few years ago, our private investment pool has the doors opened to a select few people to invest.			
Add your two cents			
11.06.2010 > HYIP.COM - The confrontation is over			
RSS of CherryShares			
OrbisTrends	Status: PAYING Our Investment: \$3550 Min/Max: \$1 - \$50000 Referral: 0.00%	Monitored: 161 days Profit: 0.50% - 3.47% daily Period: up to 120 days Withdrawal: Manual	User Rating: ☆☆☆☆☆ (6 users) Our Rating: ☆☆☆☆☆ ROI: 48% NOT IN PROFIT HYIPRANK: 2 / 1856
OrbisTrends is Computerized Logistics (TM) powered privately held financial company engaged in trading world market commodities, such as all markets-stocks, foreign currencies, ETFs, e-Minis, and mutual funds.			
Add your two cents			
25.09.2010 > OrbisTrends.com Weekly Account Statements			
RSS of OrbisTrends			
Plex Fund	Status: PAYING Our Investment: \$3150 Min/Max: \$25 - \$1000000 Referral: 0.00%	Monitored: 134 days Profit: 12.60% - 15.00% daily Period: up to 10 days Withdrawal: Instant	User Rating: ☆☆☆☆☆ (113 users) Our Rating: ☆☆☆☆☆ ROI: 121% PROFITABLE HYIPRANK: 3 / 1856
PlexFund is one of the financial services providers and is the best way for connecting you to the global markets, with minimum risk . We provide a safe place for you while investing the amounts you choose to invest . In short , we aim to deliver			
Administrator of this program did not submit any news			
RSS of Plex Fund			

