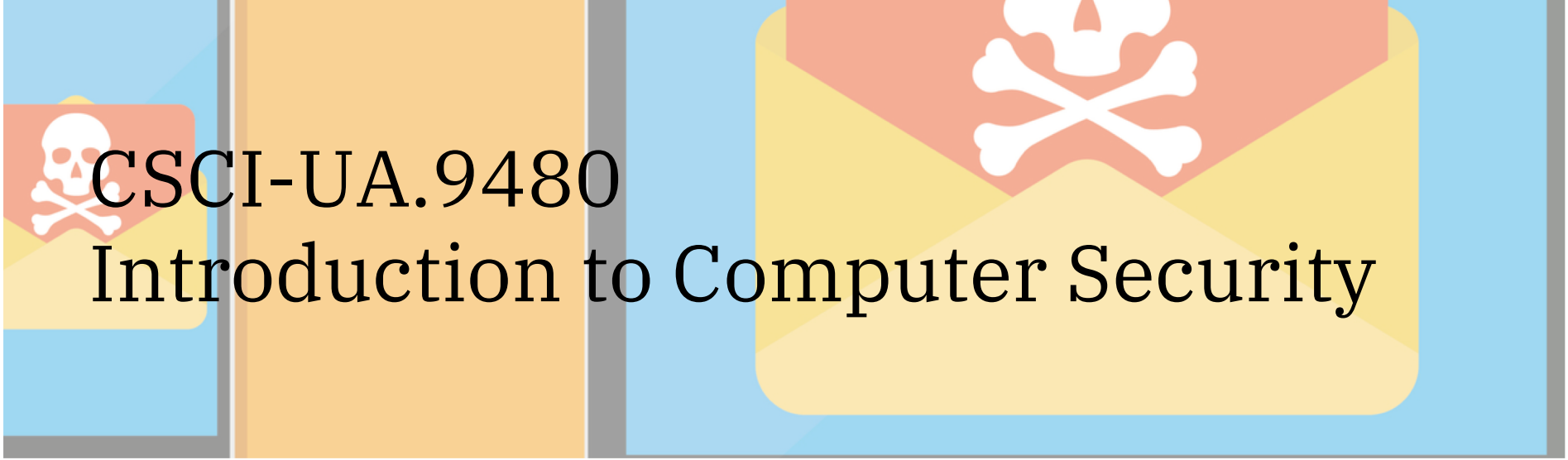


CSCI-UA.9480
Introduction to Computer Security

NYU

Session 4.5
Spam and Abuse

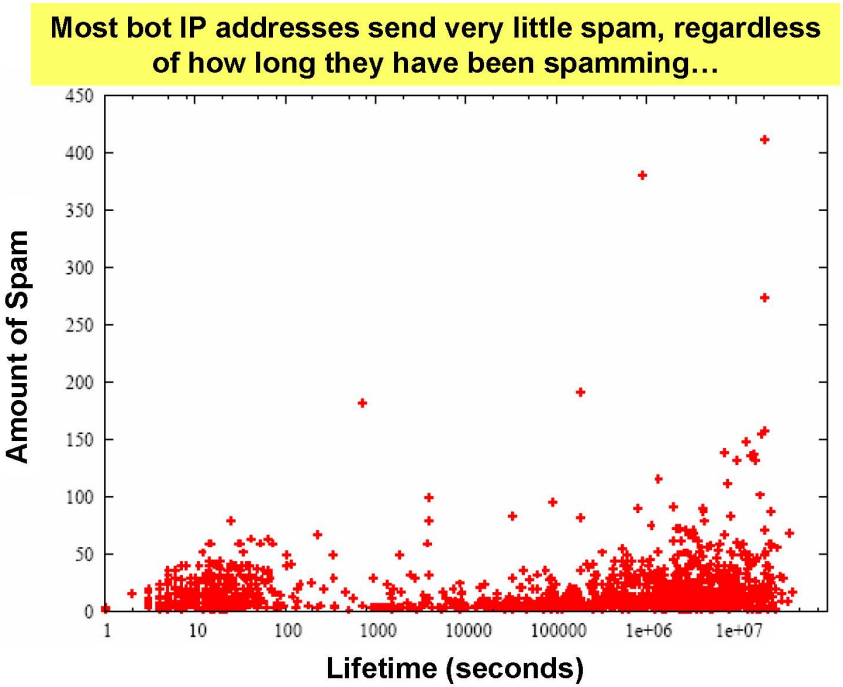
Prof. Nadim Kobeissi

What is spam?

Based on slides by Vitaly Shmatikov and Joe Bonneau.

Why hide sources of spam?

- Many email providers blacklist servers and ISPs that generate a lot of spam.
  - Use info from spamhaus.org, spamcop.net
- Real-time blackhole lists stop 15-25% of spam at SMTP connection time.
  - Over 90% after message body checks
- Spammers' objective: evade blacklists.
  - Botnets come very handy!



CAN-SPAM Act of 2003.

- Legal solution to the problem.
  - Bans email harvesting, misleading header information, deceptive subject lines, use of proxies
  - Requires opt-out and identification of advertising
  - Imposes penalties (up to $11K per violation)

FTC (Federal Trade Commission) report on effectiveness (Dec 2005)

- 50 cases pursued in the US.
- No impact on spam originating outside the US (60%.)
- Open relays hosted on botnets make it difficult to collect evidence.

Example: McColo botnets.

- McColo was a San Jose-based hosting provider. Hosted command-and-control servers of the biggest spam botnets.
    - Rustock, Srizbi, Mega-D, Pushdo/Cutwail, others.
- Disconnected by upstream providers on Nov 11, 2008 ⇒ 75% reduction of spam worldwide.
    - Didn’t last long – increased again quickly.
- Resurrected for 12 hours on Nov 20, 2008.
    - Through backup connection (soon terminated.)
    - During this time, 15MB/sec of traffic to Russia – botmasters getting data to regain control of botnets.

A closer look at spam.

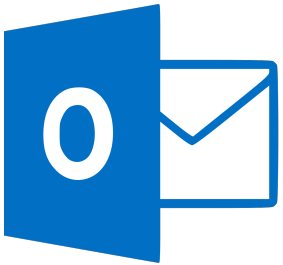
```
Received: by 10.78.68.6 with SMTP id q6cs394373hua;
                  Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Received: by 10.90.113.18 with SMTP id l18mr17307116agc.1171291410432;
                  Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Return-Path: <wvnlwee@aviva.ro>
Received: from onelinkpr.net ([203.169.49.172])
             by mx.google.com with ESMTP id
30si11317474agc.2007.02.12.06.43.18;
             Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Received-SPF: neutral (google.com: 203.169.49.172 is neither permitted nor
             denied by best guess record for domain of wvnlwee@aviva.ro)
Message-ID: <20050057765.stank.203.169.49.172@ASAFTU>
From: "Barclay Morales" <wvnlwee@aviva.ro>
To: <raykwatts@gmail.com>
Subject: You can order both Viagra and Cialis.
```

Methods to prevent spoofing.

- **SPF** (Sender Policy Framework)
  - Upon receiving email with FROM example@domain.com, query DNS for all IP addresses in domain.com.
  - If sender IP is in resulting list, pass.
  - Else, bounce back to domain.com.
  - Spammers can flood domain.com this way.
- **DKIM** (DomainKeys Identified Mail)
  - Public keys stored in DNS.
  - Sender signs with private key, add “DKIM-Signature” to header.
  - Recipient uses sender’s public key to check “DKIM-Signature”.
  - Prevents tampering and fraudulent emails.
- **DMARC** (Domain-based Message Authentication, Reporting, and Conformance)
  - Policy on what to do if message fails SPF or DKIM.

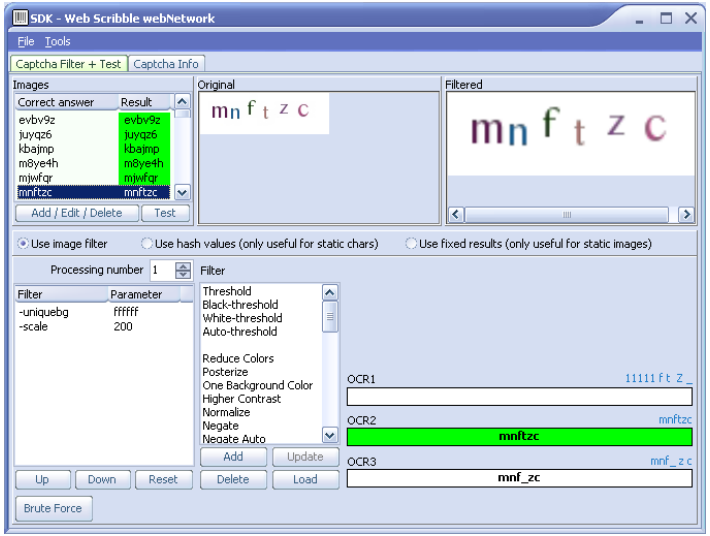
Webmail spam.

- Idea is that it's not feasible to blacklist a major webmail provider such as Gmail.
  - Depend on password reuse.
  - Find out ways to create accounts in bulk.
- Defenses: captcha, phone verification...

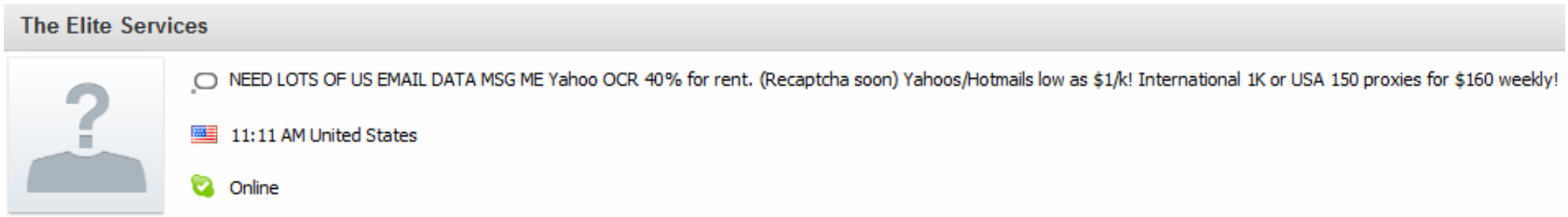


iCloud

Getting around verification methods.



Get your fresh webmail accounts!



Damon McCoy: you are selling [redacted] accounts for $1/k?

what quantity needed for that price?

The Elite Services:
$4 per k for 10k - 100k.
$3 per k for 100k - 1 million.
$2 per k for 1 million - 2 million.
$1.50 per k for 2 million+.

Spam issues at LinkedIn.

- LinkedIn did a 2016 study on “Online Social Network (OSN)” Security.
- Identified issues: fake accounts, stolen accounts, fraud, scams, spam, impersonation, scraping, stealing data, fake news.

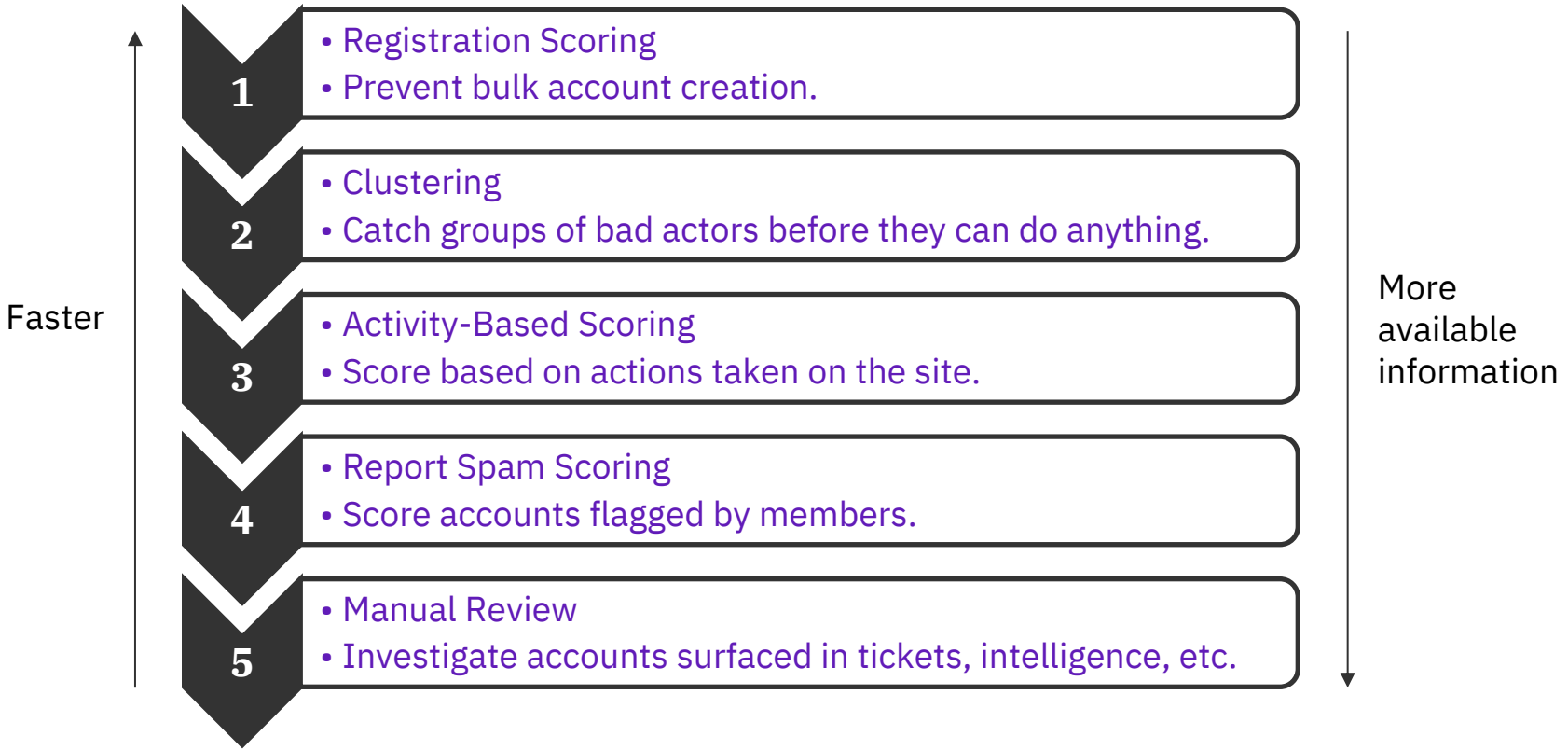
Problem: Malicious actors try to scam members and steal data.
Why is it hard? Adversary changes constantly, defense must adapt automatically.
Team vision: Classify every profile and action on LinkedIn as legitimate or abusive.

Spam issues at LinkedIn.

Problem: Malicious actors try to scam members and steal data.
Why is it hard? Adversary changes constantly, defense must adapt automatically.
Team vision: Classify every profile and action on LinkedIn as legitimate or abusive.

- Every time a user makes a request, it goes through a classifier (trained on things like IP address, patterns.)
- The request is either accepted and sent on to LinkedIn, or rejected.

LinkedIn's funnel of defenses.



Notes about clustering.

- Step one: identify attributes to cluster based on.
- Step two: perform clustering.
- Step three: score each cluster.

1. Define minimum cluster size.
2. Label each cluster as “bad” or “good”.
3. Go through standard binary classifier training procedure.
4. Score clusters online or offline.
5. Propagate cluster label to individual members.

Clustering and tainting.

- If a cluster is scored as bad, “taint” the cluster identifier: all new requests that come from that cluster (for some time) will be marked as “bad.”

- 70% “bad” actors in a cluster is not good enough!
- Some propagations from cluster labels to individuals can be inaccurate (check seniority, etc.)

Removing the “profit” element from spam.

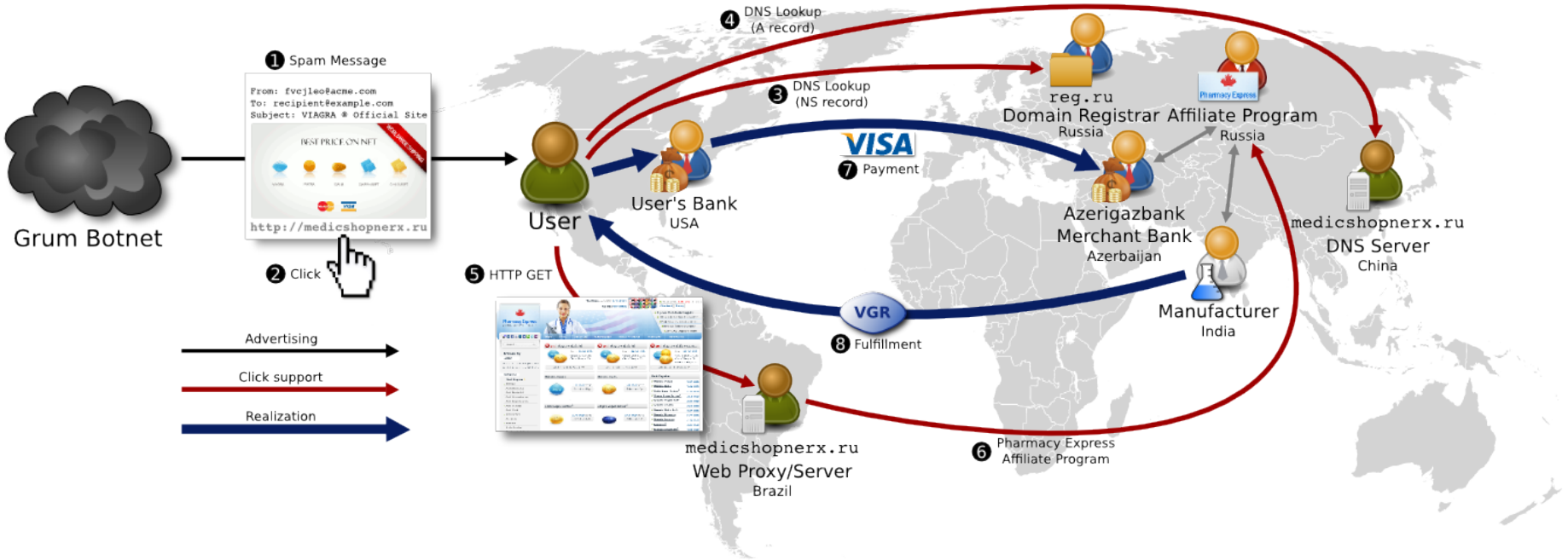
- Deterring profit-motivated attackers is like disrupting a business process.
- Raising attack cost, reducing expected gains.

Removing the “profit” element from spam.

- Deterring profit-motivated attackers is like disrupting a business process.
- Raising attack cost, reducing expected gains.

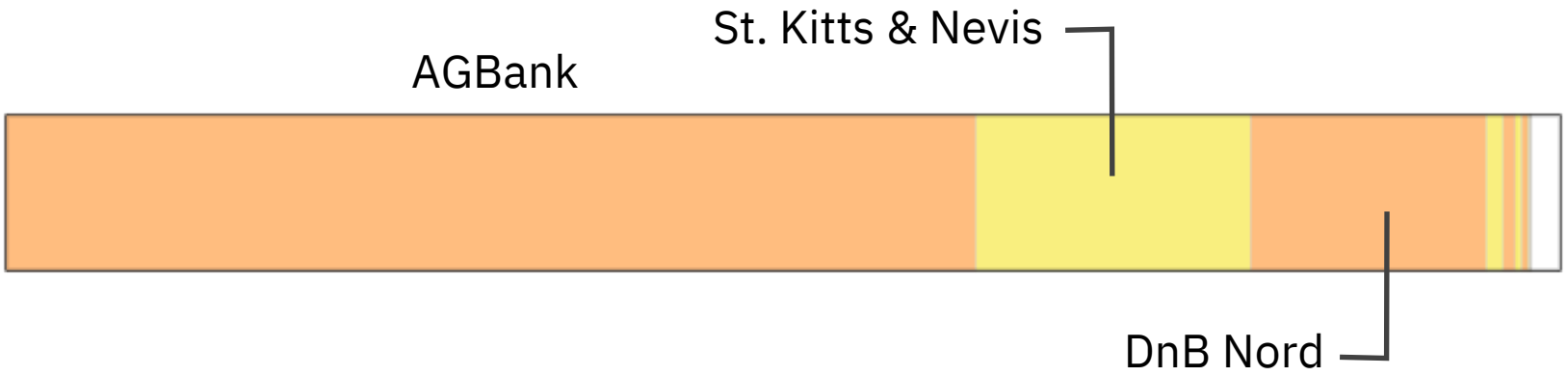
- Actors
  - Adversaries
  - Victims
  - Defenders
- Incentives/Costs
- Capabilities
- Relationships

“Pharmacy spam” value chain.



A closer look at the banks (late 2010.)

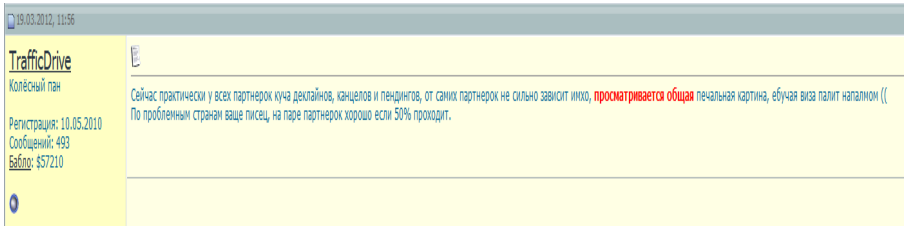
- Low diversity: 3 banks cover 95% of spam.
- High switching cost: in-person account creation, due diligence, delays, up-front capital…



“Pharmacies” accepting US Visa in 2011.

“Pharmacies” accepting US Visa today.

Summary: business disruption is effective.



"Right now most affiliate programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program imho, there is a general sad picture, fucking Visa is burning us with napalm (for problematic countries, it's totally fucked, on a couple of programs you're lucky if you get 50% through)."

Next time: Economics, Ethics and Law

The first section of Part 5 of this course: Security and Society.

5.1