



Electronic payments in the Netherlands

The Dutch approach on Cybersecurity

Gijs Boudewijn
Deputy General Manager

Vienna
May 19th 2015

Agenda



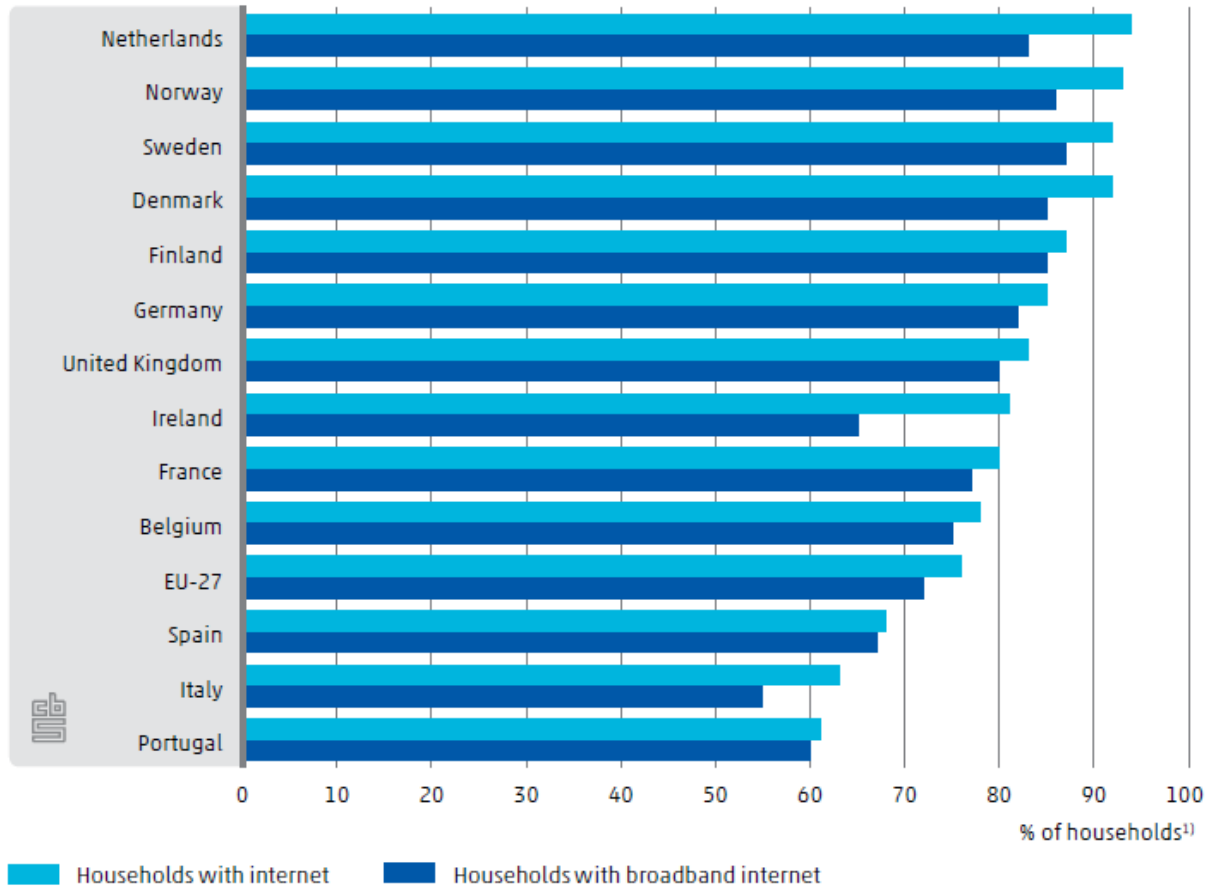
- Facts and figures
- Fraud developments in the Netherlands
 - Situation and trends
- Trends and developments
 - Mobile banking, mobile payments
- The Dutch approach, 'working together works better'
 - Shared services for the Dutch banks
 - Risk Management services of the Dutch Payments Association

Some facts



- The Netherlands has 12.3 million Internet users.
- 94% of households in the Netherlands have at least one computer. This is the second highest rate in the world.
- The Dutch are heavily using innovative services;
 - 95% of young people are intensively using social media (Twitter, Facebook).
 - Bitcoin
- Netherlands is a leader in the use of Internet banking in Europe.
- Approximately 10 million Dutch bought one or more times online (using iDEAL).
- In 2014 there were some 180 million iDEAL transactions

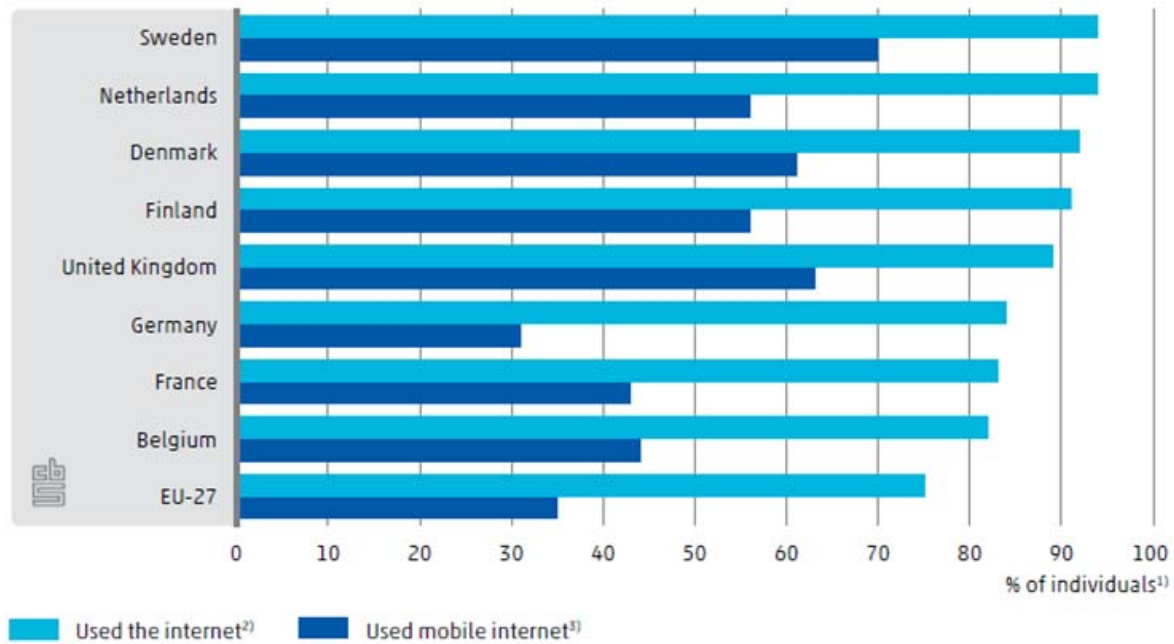
Households with (broadband) internet



Source: Eurostat.

¹⁾ Private households with at least one person aged 16 up to and including 74 years.

Usage of mobile internet



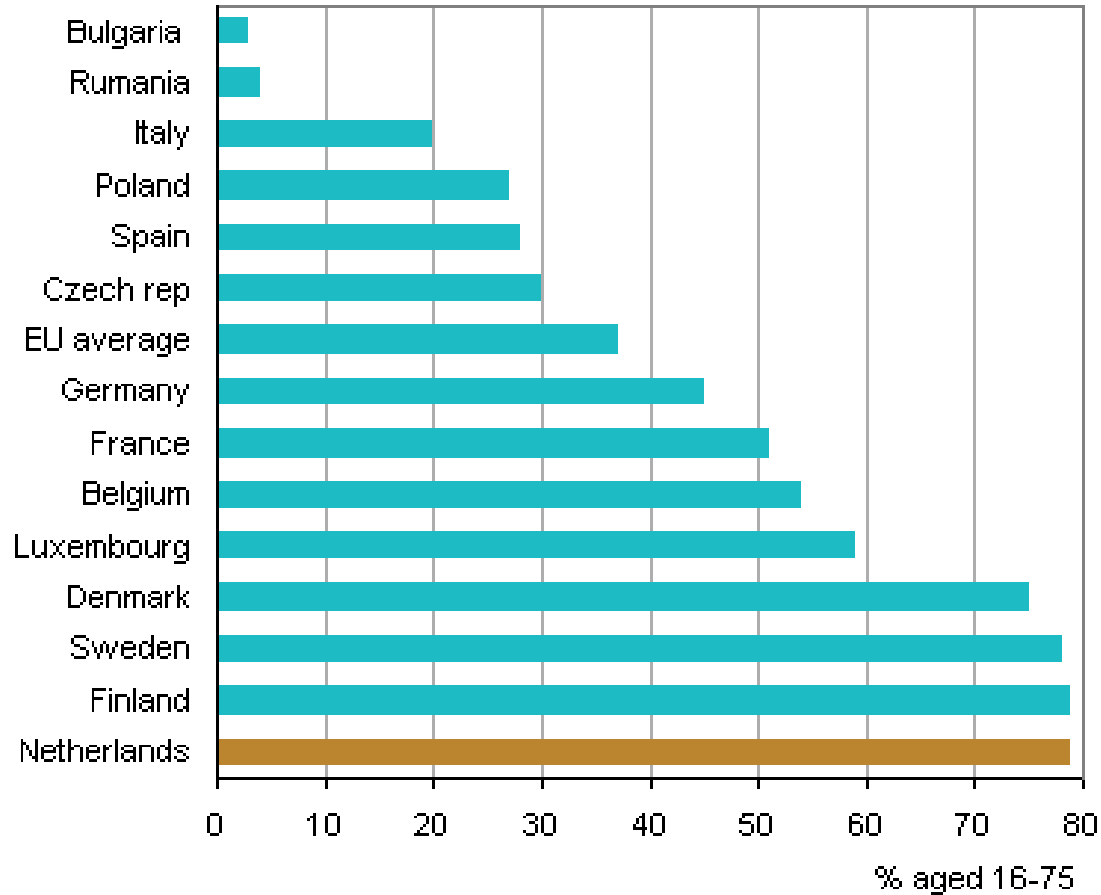
Source: Eurostat.

¹⁾ Individuals aged 16 up to and including 74 years.

²⁾ Used the internet in the twelve months prior to the survey.

³⁾ Used a mobile device, such as a smartphone, laptop or tablet, to access the internet.

Internet banking in EU countries



Fraud developments in the Netherlands



What caused the trend change ?

Skimming

- EMV migration (1-1-2011 EMV compliant)
- Collaboration
 - Information sharing between Dutch banks
 - Vendors, Payment Service Providers,
 - Retail, gasoline sector, parking sector
 - Police & public prosecutor

- Geo blocking
- Time to relax ?



What caused the trend change?

Internet banking



- Education consumers & end-users,
- Creating awareness
- Individual measures Dutch Banks
 - Malware protection on pc's
 - What You See Is What You Sign for authentication and autorisation
 - Transaction Monitoring
 - Detection and blocking of fraudulent transactions
- Sharing and learning



Cyber threats



- Phishing (phone and email)
 - Adapted to recent events (DDoS, malfunction/failures)
 - Personalized (spear phishing)
 - Demanding immediate action
- Malware
 - On desktop computer
 - Windows XP
 - Mobile apps misuse
- New Modus Operandi
 - Misusing payments schemes
 - prepaid credit
 - Misleading consumers

Decrease of fraud is only one aspect

- Reputational damage is becoming more important
 - DDoS attacks april 2013
 - Availability of internet banking
 - Availability of mobile banking
 - Resilience of payments infrastructures
 - Leading to legal requirements
 - must be further optimized



Oekraïense hackers leggen NAVO-websites plat
Datum: 16 maart 2014 08:35
Dat verklaart de club op zijn website. De club heeft de aanval uitgevoerd omdat de hackers het niet eens zijn met de bemoeienis van de NAVO ... ▶



Fraude betalingsverkeer daalt fors
Datum: 11 maart 2014 14:48
Het is het tweede achtereenvolgende jaar dat de kosten door fraude in het betalingsverkeer dalen. Dat blijkt dinsdag uit cijfers van de Nederlandse... ▶



Grootste DDoS-aanval ooit uitgevoerd in Europa
Datum: 12 februari 2014 16:44
Dat laat Cloudflare, een beveiligingsbedrijf voor bedrijven, weten. Een onbekende klant van Cloudflare is aangevallen. Het is alleen bekend... ▶



ING kampt met vier storingen in drie dagen
Datum: 5 februari 2014 08:38
Dat laat een woordvoerder aan NUtech.nl weten. Volgens ING gaat het om losstaande incidenten. Er zou ook geen sprake zijn van een DDoS-aanva... ▶



ING internetbankieren na storingen weer bereikbaar
Datum: 4 februari 2014 18:24
Internetbankieren van ING had vanochtend zowel vanuit de browser als via mobiele apparaten last van vertragingen in de transacties. In de middag wa... ▶

Trends and developments

- Mobile banking
- Mobile payments
- PSD2
- Access to account
- Instant payments



Chance or Threat?

Working together, the Dutch approach



- **Dutch Banks do not compete on security**
- FI-ISAC, Financial Institutions Information Sharing Analysis Center
 - Monthly and quarterly meetings
 - Sharing cyber security incidents and trends
 - Including Government, Police and Public Prosecution
- Working Group Security
 - Impact security on society
 - Strategic alignment with the Dutch Central Bank, Important stakeholders for payments
- ECTF, Electronic Crime Task Force
 - Banks, Dutch police and Public Prosecutor



Working together, the Dutch approach



- CMIS, Cybercrime Monitoring & Investigation Service
 - Analysis of banking malware, trojans
 - Notice and Take down of phishing sites
 - Trends and early information of new developments
- Banking Liasion officer at National Cyber Security Centre, ensuring Public Private Partnership
- AMI, Account Monitoring Information
 - Sharing rogue accounts
 - Sharing Money mule information



Shared Services Risk Management

Dutch Payments Association



- Strategic alliance Radboud University of Nijmegen
- Skimming discovery and blocking centre Equens
- Certification of payment terminals and payments service providers involved in the payment chain
- Risk analysis and Privacy Impact Assessments
- Publication of fraud figures and trends
- Consumer education
- Facilitating and participating FI-ISAC and Workgroup Security
 - Chairing EU-FI-ISAC
- Crisis management on payments schemes
- Executing and implementing projects
 - Showing availability status internet banking and iDEAL
 - DDoS exercises with financial private and public sector

