# Tentamen Capita Selecta Bedrijfsinformatica (CSBI)

31/05/2004, 09:30-12:30

Naam:
Studentnummer:

Dit tentamen bevat één vraag over je eigen paper (17 punten), twee vragen over gastcolleges (23 punten), en twee reviews van papers (30 punten per review). Je cijfer bepaalt 40% van het eindcijfer van het vak CSBI.
Je mag je antwoorden in het Nederlands óf in het Engels schrijven.
Je mag bij dit tentamen geen gebruik maken van ander materiaal en/of resources dan dit tentamen.
Het is zeer belangrijk dat je handschrift **goed leesbaar** is. Als dat niet mogelijk is ivm dyslexie, vermeld dit graag bij het begin van je antwoorden.

1. Deze vraag gaat over de door jouw ingeleverde paper.
    a. Wat is de stelling van je paper? (2 punten)
    b. Geef kritiek op je eigen stelling (niet op de vraag of de stelling wel of niet klopt!). Hoe kan je stelling verbeterd worden? (5 punten)
    c. Geef **twee verschillende** argumenten die je redenering (argumentatie) tegenspreken (en dus ook je claim). (10 punten)

Vragen 2 en 3 gaan over de gastcolleges, verzorgd door Frank Boterenbrood en Dick Kuijl.

2. Leg het begrip *alignment* uit, zoals besproken in beide gastcolleges. (5 punten)
3. Stel de ICT afdeling van KLM wil een nieuw Web-enabled wereldwijd reserveringssysteem introduceren.
    a. Welke taken en verantwoordelijkheden heft de CIO in dit project? (8 punten)
    b. Welke partijen binnen KLM zijn betrokken bij dit project (3 punten)? Beschrijf een mogelijk krachtenveld tussen deze partijen. (7 punten)

4. Bespreek de twee bijgevoegde artikelen met de bijgevoegde beoordelingformulieren (de formulieren zijn in het Engels, maar je mag je antwoorden in het Nederlands schrijven).

# Vertrouwen in de e-business: rol van de verkoper-klantinteractie

**Auteur**

Vrije Universiteit van Amsterdam, Nederland
email@few.vu.nl

## Abstract

Voordat een potentiële klant overgaat tot aankoop bij een e-business dient er vertrouwen te zijn. Deze paper geeft aan hoe een nieuwe of minder bekende e-business het vertrouwen kan verkrijgen van een klant om zo een plaats in de markt te realiseren. Verkoper-klantinteractie wordt gezien als de belangrijkste factor hiertoe, aangezien de potentiële klant uit de interactie het begrip en de zorg van de e-business voor de klant afleidt. Uit onderzoek is gebleken dat mensen die het internet opgaan om iets te kopen zich al hebben neergelegd bij risico's die bestaan bij het online zaken doen; branding speelt op langere termijn en betrouwbaarheidskenmerken (trustseals) moeten eerst zelf vertrouwen opbouwen. Deze drie factoren hebben dus minder invloed dan de verkoper-klantinteractie op het opbouwen van het vertrouwen in een nieuwe of minder bekende e-business.

## Inleiding

Tegenwoordig wordt er steeds meer gekocht via internet. Uit een meting van de ICT Consumer Monitor™ van Heliview blijkt dat de helft van de huishoudens met een internetaansluiting in 2003 een online aankoop of reservering heeft gedaan, tegen percentages van 39% in 2002 en 30% in 2001 [1]. Electronic business is het concept dat het proces van kopen, verkopen of uitwisselen van producten, diensten en informatie via computernetwerken, inclusief internet, beschrijft [2]. Deze paper richt zich op Business-to-Customer e-businesses.

Vertrouwen in de e-business wordt gezien als de belangrijkste factor voor het wel of niet overgaan tot een aankoop [3][4]. Vertrouwen kan in dit verband worden omschreven als "het geloof of de verwachting dat de verkoper zijn woord of belofte nakomt en geen misbruik maakt van de kwetsbaarheid van de klant" [3]. Om dit vertrouwen bij de klant te creëren, kan de e-business zich op verschillende punten richten: verkoper-klantinteractie, beveiligings- en privacygarantie, branding en betrouwbaarheidskenmerken [3][4]. Hoe kan een nieuwe of minder bekende e-business de concurrentiestrijd aanbinden met de reeds 'gevestigde' e-businesses en de potentiële klant overhalen om tot aankoop over te gaan?

In deze paper wordt gesteld, dat een nieuwe en/of minder bekende e-business zich, om zijn bedrijf neer te zetten tussen de e-business-concurrenten, vooral moet concentreren op de verkoper-klantinteractie om het vertrouwen te verkrijgen van een potentiële klant, zodat deze overgaat tot de eerste aankoop.

## Verkoper-klantinteractie

Onder verkoper-klantinteractie wordt verstaan: de interactiemogelijkheden tussen de klant en de verkoper middels de navigatiemogelijkheden op de website, mogelijkheden voor zoekopties en personalisatie, de gebruikersondersteuning en de 'cosmetica' (lay-out) [3]. Wanneer een klant op de website komt, is het eerste contact in de relatie tussen klant en e-business de user-interface. Aan de hand van de beschikbare informatie en kenmerken vormt de klant een eerste impressie van de webwinkel en haar betrouwbaarheid. In deze fase

heeft de e-business de gelegenheid om de klant te overtuigen van haar betrouwbaarheid. Dit is te bereiken door beschikbaarheid van informatie en door zoekopties om de potentiële klant de informatie op te kunnen laten zoeken die men wil inzien. De aanwezigheid van mogelijkheden als personalisatie, mogelijkheden tot het uitoefenen van controle op de website en navigatie door de potentiële klant en gebruikersondersteuning hebben een belangrijke invloed op de indruk en beleving van een potentiële klant.

- Een professioneel voorkomen, prettige navigatie, duidelijke website-structuur, consistentie en transparantie tijdens transacties worden door de klant uitgelegd als een teken van begrip van en respect voor de consument, wat leidt tot vertrouwen in de verkoper.
- Personalisatie kan leiden tot betere aansluiting op de behoeften van een klant door vooruit te lopen op hun behoeften en gedragingen. Dit leidt tot hogere tevredenheid van de klant en dit leidt weer tot hoger vertrouwen in de verkoper.
- Gebruikersondersteuning en mogelijkheden tot het uitoefenen van controle op de website en navigatie zijn: de toegankelijkheid van informatie over navigatie (bijvoorbeeld middels FAQ's) en de stadia in het koopproces, controle over persoonlijke gegevens en bevestigingsberichten na opdrachten door de klant of foutmeldingen. Deze factoren legt de klant uit als begrip en zorg door de e-business voor de klant. Hoe meer controle de verkoper aan de potentiële koper biedt, des te meer vertrouwen deze krijgt [3].
- Uit onderzoek [4] is gebleken dat internetgebruikers toegang wensen tot feiten als wie de website runt, identificatie van de bronnen van informatie en type informatie (advertenties duidelijk apart van overige informatie), de frequentie van updates en de datum van de laatste update. Daarbij wenst de klant transparantie over het bedrijf via de missie, visie en bereikbaarheid en informatie over de service en klantgerichte activiteiten zoals beschreven in de algemene verkoopvoorwaarden. In een onderzoek van Fogg werd hierbij gewezen op het nut om de webwinkel te ontwerpen als ware het een fysieke winkel. Deze zou geïmiteerd kunnen worden, door het fysieke adres te geven en het plaatsen van foto's van de medewerkers.

De verstrekte informatie in combinatie met het gemak en de efficiëntie waarmee klanten bij deze relevante informatie kunnen komen op de website van een bedrijf, heeft invloed op het gevoel van de klant om controle te hebben en hoe meer controle de klant heeft over zijn persoonlijke en bestellinggegevens op de website, hoe groter het vertrouwen dat de klant heeft in de verkoper [3].

Onderzoek van Bellanger [5] ondersteunt de stelling dat website-attributen als gemak, plezierig gebruik en 'cosmetica' belangrijker zijn dan zaken betreffende privacy en beveiliging. Uit dat onderzoek komt namelijk naar voren, dat gemak, plezierig gebruik en 'cosmetica' hoger gewaardeerd worden dan privacy- en beveiligingsverklaringen. De onderzoeksresultaten geven aan dat de website-kwaliteit (navigatiemogelijkheden en 'cosmetica') significant gerelateerd is aan de koopintentie. Vanuit de bestaande intentie van de klant, staat de website-kwaliteit in positieve relatie met de koopintentie en wakkert het gedrag aan indien de kwaliteit als positief wordt ervaren.
EuroClix is een gratis dienst die via e-mail en bezoek op de EuroClix-website persoonlijke en praktische informatie verstrekt over onderwerpen waarin de deelnemer geïnteresseerd is. Dit e-mailmarketingsysteem werd naar aanleiding van gebruikerstesten op het gebied van interactiekenmerken geheel herzien in de vormgeving. Een casestudy over Euroclix [7] bracht aan het licht dat deze e-business een succes werd door het herzien van de verkoper-klantinteractie.

## Beveiligings- en privacyverklaringen

Een e-business heeft een technologieplatform nodig om de website en activiteiten van bezoekers op de website te ondersteunen en de systemen en data te beveiligen. Deze technologie richt zich onder andere op de bescherming van het computersysteem van de klant en de verkoper en (klant)informatie die tijdens het bezoek uitgewisseld wordt (privacy).

Derden mogen hier geen toegang toe hebben en daarnaast dient gegarandeerd te worden dat informatie op dezelfde manier aankomt als dat hij verzonden is (integriteit).

Een verkoper is verantwoordelijk voor de informatie die op de site geplaatst en verzameld wordt en daarnaast voor het afronden van de transacties en niet misbruiken van klantendata. Voor een bezoeker van een website is het echter moeilijk in te schatten of een verkoper dit zal nakomen. Om het vertrouwen hierin te bewerkstelligen, dan wel te verhogen, worden door de verkoper beveiligings- en privacyverklaringen opgesteld [3]. De onderzoeksresultaten van Bellanger [5] geven aan dat privacy en beveiliging significant gerelateerd zijn aan de koopintentie. Echter, vanuit de bestaande intentie van de klant, hebben privacy en beveiliging een negatieve relatie met de koopintentie, wat betekent, dat zij de koopintentie kunnen doen afnemen bij een negatieve ervaring, maar niet doen toenemen bij een positieve ervaring. De reden die in het onderzoek wordt gegeven, is dat de klanten welke hebben besloten online een aankoop te doen zich al hebben neergelegd bij het ongemak en/of wantrouwen gebaseerd op privacy en beveiliging. Bellanger gaat nog verder en vermeldt dat prominente privacy- en beveiligingsindexen zelfs als hindering kunnen worden ervaren op de voorkeuren op het gebied van comfort en gemak.

## Branding

Bij branding wordt er een merkbeeld gevormd, waarbij het bedrijf en zijn producten een identiteit krijgen waardoor ze worden onderscheiden van concurrenten [3]. Branding is gericht op het in stand houden en verhogen van vertrouwen in, in dit geval, de e-business. Het proces tot merkbeeldvorming heeft tijd nodig en is gebaseerd op ervaringen van bezoekers/klanten met de e-business. Het merkbeeld wordt mede verkregen door het gezamenlijke beeld wat bestaande klanten hebben gevormd van het bedrijf. Aangezien branding over langere termijn wordt opgebouwd en kan worden ingezet voor het wekken en verstevigen van vertrouwen is het geen middel om in te zetten voor nieuwe of minder bekende e-businesses.

## Betrouwbaarheidskenmerken

Er bestaan betrouwbaarheidskenmerken (trustseals) om garanties te geven over de activiteiten en het beleid van e-businesses. Onderzoek [6] in het buitenland kwam tot de conclusie, dat slechts eenderde van de bezoekers het betrouwbaarheidskenmerk herkende en dat van deze groep slechts bij de helft van de mensen hun vertrouwen toenam. In andere landen werd het betrouwbaarheids-kenmerk helemaal niet herkend. De P3P (W3C's Platform for Privacy Preferences) meldt hierbij dat de merken geen garantie bieden dat het beschreven beleid van de e-business hun daadwerkelijke handelwijze weergeven. De P3P geeft aan dat degenen die het betrouwbaarheidskenmerk toekennen geen onafhankelijke partij zijn en in het belang van de e-business werken. Ook uit het onderzoek van Princeton Survey Research Associates [4] blijkt dat merken als weinig belangrijk worden gezien door de website-bezoekers. Hetzelfde geldt volgens dit onderzoek voor awards en certificaten. Als belangrijke reden voor het niet hechten van waarde aan de merken, wordt de wildgroei gezien die in het begin van het Web heeft plaatsgevonden. Onderzoek van Kuchinskas [5] komt tot de conclusie dat de betrouwbaarheidscertificaten zelf in eerste instantie aan vertrouwensopbouw moeten doen. Uit de casestudy over Euroclix kwam naar voren dat betrouwbaar-heidskenmerken slechts effectief zouden zijn als ze werden afgegeven door een organisatie welke bekend is en vertrouwen heeft, zoals de Consumentenbond [7].

## Conclusie

Om vertrouwen bij de klant te creëren, kan de e-business zich op verschillende punten richten: verkoper-klantinteractie, beveiligings- en privacygarantie, branding en betrouwbaarheidskenmerken. Een professioneel voorkomen, prettige navigatie, duidelijke website-structuur, consistentie en transparantie tijdens transacties, evenals personalisatie en

gebruikersondersteuning geven de klant een gevoel van controle over zijn transacties en gegevens en zorg vanuit de verkoper. Vanuit de bestaande intentie van de klant, staat de website-kwaliteit in positieve relatie met de koopintentie en wakkert het gedrag aan indien de kwaliteit als positief wordt ervaren. Beveiligings- en privacyverklaringen hebben minder invloed op het doen van een eerste online aankoop, aangezien klanten welke hebben besloten tot een online aankoop, zich al hebben neergelegd bij het ongemak en/of wantrouwen gebaseerd op privacy en beveiliging. Branding betreft een beeldvorming die over langere termijn wordt opgebouwd en kan worden ingezet voor het wekken en verstevigen van vertrouwen. Het is echter geen effectief middel om in te zetten voor nieuwe of minder bekende e-businesses. Wat betreft betrouwbaarheidskenmerken kan gesteld worden, dat zij eerst zelf vertrouwen moeten verkrijgen en uit onderzoek blijkt dat mensen de garanties vaak niet herkennen. Daarbij wordt gesteld, dat in het verleden vrij eenvoudig betrouwbaarheidskenmerken verkregen konden worden en deze niet altijd door onafhankelijke partijen werden toegekend.

Op basis van deze argumenten is in deze paper gesteld, dat een nieuwe en/of minder bekende e-business zich, om zijn bedrijf neer te zetten tussen de e-business-concurrenten, vooral moet concentreren op de verkoper-klantinteractie om het vertrouwen te verkrijgen van een potentiële klant, zodat deze overgaat tot de eerste aankoop.

## References

[1] Heliview online beschikbaar: http://www.heliview.nl/news/bericht103.html

[2] Turban, E., King, D., e.a. (2004): Electronic Commerce – A Managerial Perspective 2004, Pearson Education International, Inc, Upper Saddle River, New Yersey 07458.

[3] Ildemaro Araujo, Ivan Areujo (2003): Developing Trust in Internet Commerce (Toronto, Ontario, Canada)

[4] Princeton Survey Research Associates (2002): A Matter of Trust: What Users Want From Web Sites - Results of a National Survey of Interne Users for Consumer WebWatch. Online beschikbaar: http://www.consumerwebwatch.org/news/1_abstract.htm

[5] Bellanger, F. Hiller J.S., Smith W.J. (2002) Trustworthiness in electronic commerce: the role of privacy, security, and site attributes,

[6] Patton, M., Jøsang, A., (2004) :Technologies for Trust in Electronic Commerce, Electronic Commerce Research, No. 4, pp. 9–21

[7] Egger, F.N., Groot, de, B. (2000): 9th International World Wide Web Conference "Developing a Model for Electronic Commerce: An Application to a Permissive Marketing Web Site", Amsterdam 15-19 mei 2000

## Tentamen Capita Selecta Bedrijfsinformatica (CSBI)

31/05/2004, 09:30-12:30

# De menselijke factor in IT security

**Auteur**

Vrije Universiteit Amsterdam, Holland
email@cs.vu.nl

## Abstract

In deze paper zal worden bewezen dat focus op technologie alleen, niet voldoende is om security in commerciële organisaties te creëren en te waarborgen. Vervolgens zal worden aangetoond dat dit wel kan door meer aandacht dan nu het geval is in deze organisaties, te besteden aan de menselijke factor. Dit zal gebeuren aan de hand van user awareness en usability, met de daarbij behorende mogelijkheden tot verbetering.

## Introductie

Security kan worden gezien als het waarborgen van vertrouwelijkheid, integriteit en beschikbaarheid van informatie [1]. Vertrouwelijkheid staat voor de mate waarin informatie toegankelijk is voor alleen die personen die daartoe bevoegd zijn. Integriteit is de eigenschap dat informatie niet op ongeautoriseerde wijze is verandert of vernietigd. Daarnaast geeft beschikbaarheid van informatie de mate aan waarin deze, wanneer nodig, toegankelijk is voor en te gebruiken is door bevoegde gebruikers [1]. Een incident is elke handeling die een of meerdere van de drie genoemde punten schaadt of in gevaar brengt.

De menselijke factor in security, ofwel de menselijke kant van security, geeft de rol weer van de mens in het bereiken en waarborgen van security. Zoals Adams en Sasse [2] aangeven worden security mechanismen ontworpen, geïmplementeerd, toegepast, gebruikt en gekraakt door mensen.

In deze paper zullen wij aantonen dat er meer aandacht moet worden besteed aan de menselijke kant van security, om deze in organisaties te creëren en te waarborgen. Hierbij gaat het met name om commerciële organisaties en bedrijven, bijvoorbeeld banken en uitgeverijen. In tegenstelling tot de technologische kant, krijgt de menselijke kant namelijk nauwelijks aandacht in het merendeel van de huidige organisaties [3]. Echter, we willen niet aantonen dat alleen de menselijke kant van belang is.

In sectie 2 zal worden aangeven dat technologie alleen niet voldoende is om security in een organisatie te waarborgen. Vervolgens zal in sectie 3 worden ingegaan op twee belangrijke aspecten van de menselijke factor in security: user awareness en usability. Hierin zullen ook enkele mogelijkheden tot verbetering worden besproken. Afsluitend bevat sectie 4 de conclusie.

## Alleen technologie

Het grootste deel van het IT security budget in organisaties is gereserveerd voor technologische middelen [3]. Het aantal security incidenten neemt echter toe en de hiermee gepaard gaande financiële verliezen nemen niet af [4]. Dit suggereert dat technologie alleen niet adequaat is om security te waarborgen.

De jaarlijkse CSI/FBI Computer Crime and Security Survey [4] bevat de volgende gegevens: 98% van de ondervraagde organisaties hebben firewalls en 73% hebben zogenaamde intrusion detection systems, maar 36% gaf nog steeds aan dat hun systemen van buitenaf zijn binnengedrongen. Hoewel 98% van de ondervraagden anti-virus software gebruikt, wordt 82% van hen nog steeds aangevallen door virussen en wormen.

Alleen technologische security oplossingen kunnen een groot deel van de incidenten dus niet voorkomen.

## De menselijke factor

Technologische oplossingen kunnen, zoals gezien, het aantal security incidenten niet reduceren [4], daarom pleiten wij voor het zoeken naar oplossingen van andere aard. De menselijke kant van security biedt hier een mogelijkheid.

Twee belangrijke aspecten van de menselijke kant van security zijn user awareness en usability. Juist deze aspecten zijn belangrijk, omdat voor beide is aangetoond dat ze kunnen bijdragen aan een verhoging van de algehele security binnen organisaties [2].

### *User awareness*

Adams en Sasse [2] beschrijven dat gebrek aan security awareness in een organisatie, problemen kan veroorzaken die de effectiviteit van security in die organisatie doen afnemen.

Bij een gebrek aan aangereikte informatie over security maken gebruikers hierover hun eigen waardepatroon [2]. Het gevolg hiervan is dat informatie voor verschillende mensen binnen een organisatie een verschillende betekenis heeft in security opzicht. Zo kan het voorkomen dat een werknemer zich niet bewust is van de vertrouwelijkheid van de informatie in een document, waardoor deze informatie uiteindelijk beschikbaar wordt voor onbevoegden. Ook het openen van verdachte email attachments is een voorbeeld van een soortgelijk gebrek aan security awareness.

Daarnaast is er het zogenaamde "Social Engineering". Social Engineering in IT security staat voor een diversiteit aan technieken om ongeautoriseerd toegang te krijgen tot informatie, en is in veel gevallen gebaseerd op het winnen van het vertrouwen van eindgebruikers [5]. Een voorbeeld is het zich voordoen als iemand die wél bevoegd is om toegang te krijgen tot bepaalde informatie, terwijl dit in werkelijkheid niet het geval is. Social Engineering blijkt een succesvolle methode voor het verkrijgen van vertrouwelijke informatie van organisaties [5].

Ook is er het gevaar van "complacency", het blind vertrouwen op technologie. Gebruikers hebben in dit geval het gevoel dat, welke fouten ze ook maken, deze worden verholpen door technologische mechanismen of door de security afdeling. In beide gevallen is het gevoel van verantwoordelijkheid verdwenen, waardoor met name de vertrouwelijkheid van informatie in het geding komt. Meerdere niet-wetenschappelijke bronnen, zoals [6] ,vermelden complacency als een belangrijk gevaar op security gebied. Wetenschappelijke bronnen, waaronder [7], noemen echter alleen het gebrek aan verantwoordelijkheid van gebruikers.

Het verhogen van user awareness kan met name door het trainen en ondersteunen van werknemers [2, 5, 8]. Adams en Sasse [2] geven aan dat user awareness in de praktijk verhoogd kan worden door:

- Het informeren van gebruikers over bestaande en potentiële gevaren aangaande de systemen in een organisatie, de gevoeligheid van de informatie in deze systemen en de reden van deze gevoeligheid.
- Het onderhouden van het belang van security arwareness van gebruikers in een organisatie, door het detecteren en constructief oplossen van het omzeilen van security mechanismen.

Daarbij komt, zoals Kajava en Siponen [5] aangeven, dat gebruikers moet worden geleerd welke handelingen zij dienen uit te voeren in security bedreigende situaties.

### *Usability*

Allereerst moet worden opgemerkt dat usability in dit betoog valt onder de menselijke factor van security en niet onder de technologische factor. Dit geeft aan dat de aandacht op dit gebied naar de mens dient uit te gaan, maar dit neemt niet weg dat usability op de grens van beiden staat. Menselijk gedrag en menselijke beperkingen bepalen namelijk voor een groot deel het slagen of falen van technische security mechanismen.

Zo zijn ongebruiksvriendelijke security systemen niet alleen duur, maar ook ineffectief [7, 9].

Technische security mechanismen worden namelijk altijd door mensen gebruikt of ingeschakeld. In de praktijk blijkt echter dat security mechanismen vaak niet overeenkomen met menselijke beperkingen, zowel fysiek als mentaal, of met de uit te voeren taken [2, 7].

Een voorbeeld is het gebruik van passwords. Adams en Sasse [2] tonen aan dat gebruikers password mechanismen ondermijnen als deze niet overeenkomen met de taken die moeten worden uitgevoerd. Ondermijnen is in dit geval het delen of openbaar maken van passwords. Ook tonen zij aan dat als een organisatie zijn gebruikers het vormen van complexe en wisselende passwords oplegt, dit kan resulteren in uiteindelijke achteruitgang in security. Gebruikers kunnen slechts een beperkt aantal passwords onthouden. Wordt deze grens overschreden, dan schrijven gebruikers hun passwords op, of bedenken zij dusdanig simpele passwords dat deze makkelijk te kraken zijn.

Sasse, Brostoff en Weirich [7, 9] zoeken de mogelijkheid tot het verhogen van usability van security mechanismen en uiteindelijk de algehele security, in human/computer interaction. Door het betrekken van human/computer interaction in het ontwerpproces van security mechanismen, wordt er rekening mee gehouden dat gebruikers en technologie samenwerken om een taak te vervullen, zowel in fysieke als sociale context [7]. De volgende praktische, op principes uit human/computer interaction gebaseerde verbeteringen worden in de litratuur genoemd:

- Het minimaliseren van de fysieke en mentale last van gebruikers [9].
- Security mechanismen op één lijn zetten met de door gebruikers uit te voeren taken [7, 9].

Security mechanismen bevorderen de security dus niet als er geen rekening is gehouden met degenen die deze mechanismen gebruiken of inschakelen. Het vergroten van de usability zal daarentegen leiden tot verhoogde security.

## Conclusie

Er gaat veel aandacht uit naar technologische oplossingen in IT security. Technologie alleen is echter niet voldoende om security te creëren en te waarborgen. De menselijke factor in security biedt hier een mogelijkheid. Voor zowel user awareness als usability zijn een aantal mogelijke verbeteringen besproken, waaronder het trainen en ondersteunen van gebruikers en het ontwerpen van security mechanismen rekening houdend met de taak en eigenschappen van deze gebruikers. Aandacht aan user awareness en usability kan zoals aangetoond een aantal security problemen voorkomen. Om security te verhogen, zal dus meer aandacht moeten worden besteed aan de menselijke factor in security.

### Referenties

[1] International Standard ISO 7498-2 (1989): Information processing Systems - Open Systems Interconnection - Basic Reference Model - part 2: Security Architecture, Zwitserland

[2] Adams, A., Sasse, M. A. (1999): Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures, Communications of the ACM, Vol. 42, No. 12, pp. 40 – 46.

[3] GISS Ernst & Young Global Information Security Survey 2003

[4] CSI/FBI Computer Crime and Security Survey 2003

[5] Kajava, J., Siponen, M. T. (1997): Social Engineering - IT Security Threat of Informatics, http://iris.informatik.gu.se/conference/iris20/9.htm

[6] Rose, C. (2002): Business Information Security for the Business Person, http://www.itsecurity.com/papers/iomart1.htm

[7] Sasse, M. A., Brostoff, S., Weirich, D. (2001): Transforming the 'weakest link' – a human computer interaction approach to usable and effective security, BT technology journal, Vol. 19, No. 3, pp. 122 – 131.

[8] Brostoff, S., Sasse, M. A. (2002): Safe and sound: a safety-critical design approach to security, 10th ACM/SIGSAC New Security Paradigms Workshop 2001, Cloudcroft, New Mexico, September 10-13, ACM Press.

[9] Sasse, M. A. (2003): Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery, CHI 2003 Workshop on Human-Computer Interaction and Security Systems, Ft. Lauderdale, April 5

Naam:

**Title of Manuscript**: `Vertrouwen in de e-business: rol van de verkoper-klantinteractie`

**Which category describes this manuscript?**

- ❑ Practice/Application/Case
- ❑ Study/Experience Report
- ❑ Research/Technology
- ❑ Survey/Tutorial/How-To
- ❑ Other (please specify): .....

**Are the title, the abstract and the introduction appropriate? Please comment.**

| Title | Abstract | Introduction |
|---|---|---|
| ❑ Yes | ❑ Yes | ❑ Yes |
| ❑ No | ❑ No | ❑ No |

Explain:.....
.....
.....
.....
.....

**Discuss the contribution made by the manuscript**:

Explain:.....
.....
.....
.....
.....

**Rate the paper in each of the following areas (1 = low ; 4 = high):**

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Technical content | ❑ | ❑ | ❑ | ❑ | ..... |
| Business content | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....
.....
.....
.....
.....

Naam:

Vertrouwen in de e-business: rol van de verkoper-klantinteractie

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Originality of claim | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....

Statements are exaggerated YES / NO .....

.....
.....
.....
.....

| | | | | | |
|---|---|---|---|---|---|
| Clarity and Organisation | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....

| | | | | | |
|---|---|---|---|---|---|
| Writing style/Grammar | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....

## COMMENTS ON SCIENTIFIC REASONING

**Rate the paper in each of the following areas (1 = low ; 4 = high):**

**Claim:**

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Well-formulated | ❑ | ❑ | ❑ | ❑ | ..... |

.....

| | | | | | |
|---|---|---|---|---|---|
| All concepts are explained | ❑ | ❑ | ❑ | ❑ | ..... |

.....

| | | | | | |
|---|---|---|---|---|---|
| Generic (1) vs. concrete (4) | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....

**Reasoning:**

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Well-structured | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....

**Naam:**

Vertrouwen in de e-business: rol van de verkoper-klantinteractie

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Shallow (1) vs. profound | ❑ | ❑ | ❑ | ❑ | ..... |
| Enough sound examples | ❑ | ❑ | ❑ | ❑ | ..... |
| Generic (1) vs. concrete (4) | ❑ | ❑ | ❑ | ❑ | ..... |

**Conclusion**:

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Based on logical reasoning | ❑ | ❑ | ❑ | ❑ | ..... |
| Contains new elements (1=yes, 4=no) | ❑ | ❑ | ❑ | ❑ | ..... |

**Does the manuscript contain sufficient and appropriate references? Please comment.**

| | NO | | | YES | Explain |
|---|---|---|---|---|---|
| Sufficient references | ❑ | ❑ | ❑ | ❑ | ..... |
| References in conference style | ❑ | ❑ | ❑ | ❑ | ..... |
| References where appropriate | ❑ | ❑ | ❑ | ❑ | ..... |

**Suggestions for improvement to the paper**:

## Tentamen Capita Selecta Bedrijfsinformatica (CSBI)

31/05/2004, 09:30-12:30

Naam:

Vertrouwen in de e-business: rol van de verkoper-klantinteractie

**Final Recommendation**:

- ❑ Definitely accept
- ❑ Borderline
- ❑ Accept only if the following changes are made: .....
.....
- ❑ Reject (poor quality)
- ❑ Other (please specify)

Explain:.....
.....
.....
.....

**Any further confidential comments you would like to make to the editor only**

.....
.....
.....

## Tentamen Capita Selecta Bedrijfsinformatica (CSBI)

31/05/2004, 09:30-12:30

Naam:

**Title of Manuscript:** De menselijke factor in IT security

**Which category describes this manuscript?**

- ❑ Practice/Application/Case
- ❑ Study/Experience Report
- ❑ Research/Technology
- ❑ Survey/Tutorial/How-To
- ❑ Other (please specify): .....

**Are the title, the abstract and the introduction appropriate? Please comment.**

| Title | Abstract | Introduction |
|---|---|---|
| ❑ Yes | ❑ Yes | ❑ Yes |
| ❑ No | ❑ No | ❑ No |

Explain:.....
.....
.....
.....
.....

**Discuss the contribution made by the manuscript:**

Explain:.....
.....
.....
.....
.....

**Rate the paper in each of the following areas (1 = low ; 4 = high):**

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Technical content | ❑ | ❑ | ❑ | ❑ | ..... |
| Business content | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....
.....
.....
.....
.....

Naam:

De menselijke factor in IT security

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Originality of claim | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....

Statements are exaggerated YES / NO .....

.....
.....
.....
.....

| | | | | | |
|---|---|---|---|---|---|
| Clarity and Organisation | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....

| | | | | | |
|---|---|---|---|---|---|
| Writing style/Grammar | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....
.....

## COMMENTS ON SCIENTIFIC REASONING

**Rate the paper in each of the following areas (1 = low ; 4 = high):**

**Claim**:

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Well-formulated | ❑ | ❑ | ❑ | ❑ | ..... |

.....

| | | | | | |
|---|---|---|---|---|---|
| All concepts are explained | ❑ | ❑ | ❑ | ❑ | ..... |

.....

| | | | | | |
|---|---|---|---|---|---|
| Generic (1) vs. concrete (4) | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....

**Reasoning**:

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Well-structured | ❑ | ❑ | ❑ | ❑ | ..... |

.....
.....
.....

Naam:

## De menselijke factor in IT security

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Shallow (1) vs. profound | ❑ | ❑ | ❑ | ❑ | ..... |
| Enough sound examples | ❑ | ❑ | ❑ | ❑ | ..... |
| Generic (1) vs. concrete (4) | ❑ | ❑ | ❑ | ❑ | ..... |

**Conclusion**:

| | 1 | 2 | 3 | 4 | Explain |
|---|---|---|---|---|---|
| Based on logical reasoning | ❑ | ❑ | ❑ | ❑ | ..... |
| Contains new elements (1=yes, 4=no) | ❑ | ❑ | ❑ | ❑ | ..... |

**Does the manuscript contain sufficient and appropriate references? Please comment.**

| | NO | | | YES | Explain |
|---|---|---|---|---|---|
| Sufficient references | ❑ | ❑ | ❑ | ❑ | ..... |
| References in conference style | ❑ | ❑ | ❑ | ❑ | ..... |
| References where appropriate | ❑ | ❑ | ❑ | ❑ | ..... |

**Suggestions for improvement to the paper**:

.....

.....

.....

.....

## Tentamen Capita Selecta Bedrijfsinformatica (CSBI)

31/05/2004, 09:30-12:30

Naam:

De menselijke factor in IT security

**Final Recommendation**:

- ❑ Definitely accept
- ❑ Borderline
- ❑ Accept only if the following changes are made: .....
.....
- ❑ Reject (poor quality)
- ❑ Other (please specify)

Explain:.....
.....
.....
.....

**Any further confidential comments you would like to make to the editor only**

.....
.....
.....