E2 → Gestion de la relation client

ÉTUDE DE CAS TECHNIQUE

Le sujet comprend 2 parties et 12 pages numérotées.

1ère partie : environnement professionnel économique et juridique de la vente à distance.

- L'environnement juridique : la protection du consommateur
- L'espace de travail : la répartition des tâches
- L'utilisation des fichiers informatiques

2ème partie : résolution de problèmes "client" avec l'utilisation de techniques de communication écrite.

- Les messages courants : courrier individualisé
- Les messages médiatisés : e-mail

Toutes les annexes sont à remettre avec la copie

		Session **2007**		Facultatif : code
Examen **Mention complémentaire : Assistance, conseil, vente à distance**				
Intitulé de l'épreuve **E2 → Gestion de la relation client**				
Type **SUJET**	Facultatif : date et heure	Durée 3 heures	Coefficient 3	N° de page **1/12**

Mise en situation

Vous travaillez en tant que télé-conseiller(e) dans le centre de contacts de la Société DAMART situé à Roubaix.
DAMART cultive le goût du bien-être depuis plus de 50 ans et occupe une place de leader dans les entreprises de vente à distance.
Plus confortables que jamais, les qualités des productions labellisées "THERMOLACTYL" de la marque, ont conquis une clientèle toujours plus large au-delà de la France, pays d'origine.

Implantée également en Belgique, en Grande-Bretagne, en Suisse et au Japon, "DAMART" est aujourd'hui reconnue comme une référence internationale et vise désormais une place de leader européen sur le marché des séniors.

1ère partie : environnement professionnel économique et juridique de la vente à distance.

✍ *Travail à faire n° 1*

Les télé-prospecteurs sont de plus en plus sollicités sur des questions concernant la sécurisation des paiements.
Votre superviseur, Monsieur DURAND, vous demande de concevoir un mémo "Foire aux Questions" (annexe 1) à leur intention.
Pour vous aider, il vous remet la fiche n° 1 de "E-Commerce" (document A).

Complétez les réponses sur l'*annexe 1* (à remettre avec la copie).

✍ *Travail à faire n° 2*

Un poste de télé-conseiller est à pourvoir chez DAMART. Une annonce doit être rédigée.

2.1 Citez 10 qualités et/ou compétences requises pour ce poste (à rédiger sur la copie).

Pour préparer l'entretien et tester les futurs candidats à cette offre d'emploi, M. DURAND a préparé une série de questions. La société DAMART s'attache à respecter la législation en matière d'e-mailing et de protection de données personnelles.

2.2 Votre tuteur vous demande de répondre à ces questions (à rédiger sur la copie) :

- **1. Quelle différence faites-vous entre e.mailing et spamming ?**
- **2. Que signifie une adresse e.mail « opt-in » ?**
- **3. Quels sont les droits du consommateur quant à l'enregistrement d'informations personnelles, dans la base de données de l'entreprise ?**
- **4. En cas de litige, à quel organisme peut-il s'adresser ?**

2ème partie : résolution de problèmes "client" avec l'utilisation de techniques de communication écrite.

✍ *Travail à faire n° 1*

Vous êtes confronté(e) aux craintes de Monsieur MORTIER, nouveau client, domicilié au 130 rue Solférino à LILLE qui vous interroge par courriel ce jour sur le paiement en ligne et les procédures de sécurité.

À l'aide de vos connaissances et des documents B et C :

B. « Résumé d'une conversation précédente avec un client. »
C. « FEVAD. Achat en ligne comment payer en toute sécurité ? »

Rédigez un courrier individualisé à M. MORTIER sur l'*annexe 2,* répondant aux craintes de ce nouveau client. (à remettre avec la copie).

✍ *Travail à faire n° 2*

Votre superviseur vous a demandé de relancer les clients qui n'ont pas passé commande depuis six mois sur le secteur de LILLE.
Votre recherche débouche sur quelques clients sélectionnés dans le fichier (document D Extrait du fichier informatisé).

À partir du document D, vous envoyez un courriel de relance pour chacune des clientes concernées en remplissant les *annexes 3, 4 et 5.*

sécurité

E-commerce • Fiche n°1

Peut-on faire confiance au paiement en ligne ?

Saisir son numéro de carte bancaire sur Internet n'est pas encore un geste aussi anodin que tendre cette même carte à une caisse de supermarché. La crainte qui y est associée reste indiscutablement un frein à l'essor du commerce électronique. Qu'en est-il des risques réels ? Comment les amoindrir ? A qui accorder sa confiance ?

Ce que vous apprend cette fiche :

DÉCOUVERTE

▸▸ à limiter les risques d'utilisation frauduleuse de votre carte bancaire.

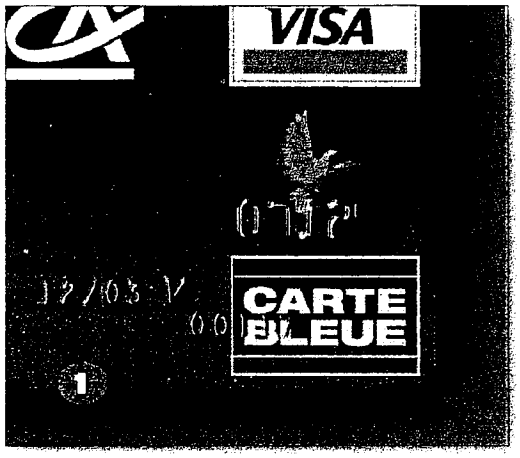
MAÎTRISE

▸▸ à contester auprès de votre banque un débit anormal.
à juger de l'intérêt des assurances complémentaires.

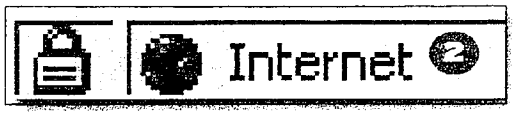
Découverte

Limitez les risques du paiement électronique

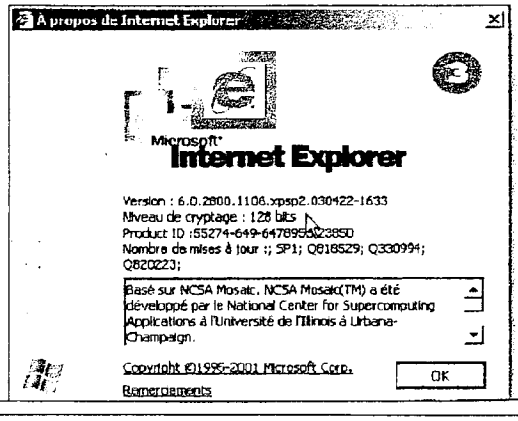
1 **Evaluez les risques.**
Le problème du paiement en ligne est lié à deux facteurs : la transmission du numéro de carte de crédit sur Internet et le stockage de ce numéro sur le site du vendeur. Dans ces deux situations, votre numéro de carte peut en théorie faire l'objet d'un piratage. En pratique, il est possible de réduire très notablement les risques en jouant sur ces deux facteurs.



2 **Vérifiez la sécurité de la transaction.**
La transmission des informations sensibles sur Internet (numéro de carte de crédit en particulier, mais aussi gestion en ligne de votre compte bancaire et autre) s'effectue dans un mode sécurisé par le protocole SSL (Secure Sockets Layer). Les informations ainsi transmises subissent des transformations mathématiques qui les rendent illisibles sans une clé de décodage. Dans ce mode, l'icône d'un cadenas fermé apparaît à droite de la barre d'état d'Internet Explorer (la barre située en bas de la fenêtre). Vérifiez que cette icône est bien présente avant de saisir et expédier votre numéro de carte bancaire sur une page Web.



3 **Vérifiez le niveau de cryptage.**
L'efficacité du protocole SSL dépend en grande partie de son niveau de chiffrement (cryptage) exprimé en bits. Les versions anciennes d'Internet Explorer ne disposaient que d'un niveau de cryptage de 40 ou 56 bits. Les versions actuelles bénéficient d'un cryptage sur 128 bits, pratiquement inviolable par des moyens conventionnels. Si vous ne disposez que d'une ancienne version d'Internet Explorer, il est temps de la mettre à jour via Windows Update. Vous pouvez accéder à ce service par le menu Démarrer, puis Tous les programmes.



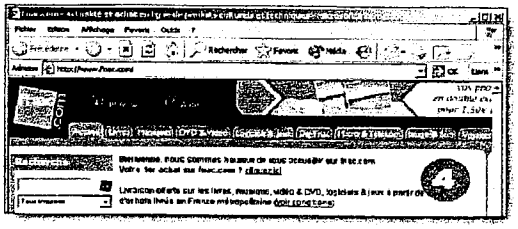
▸▸ **A SAVOIR**
Si vous restez réfractaire à l'idée de laisser votre numéro de carte bleue sur Internet, rien ne vous empêche d'opter pour une solution de paiement plus classique. De nombreux sites acceptent en effet les paiements par téléphone ou télécopie (il faudra tout de même fournir ici aussi votre numéro de carte), ou par courrier postal (envoi d'un chèque). Vous perdrez toutefois le caractère instantané de la transaction électronique.

sécurité

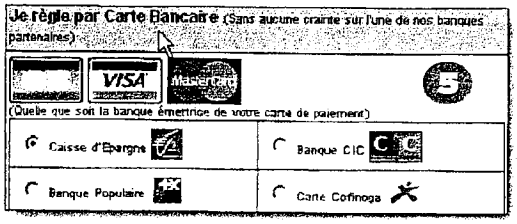
Fiche n°1 • E-commerce

Des risques partagés
Contrairement à une idée reçue, Internet n'a pas l'exclusivité des fraudes à la carte bancaire. Certains fraudeurs ont exploité le numéro de carte de crédit présent sur les facturettes délivrées par les commerçants et les distributeurs de billets pour des achats téléphoniques, par correspondance... ou sur Internet. Ce type de fraude est en passe de devenir impossible, les reçus délivrés ne mentionnant plus qu'une partie des numéros de la carte. Autre méthode de fraude : la subtilisation temporaire de votre carte chez un commerçant par un fraudeur qui vous a vu taper votre code confidentiel.

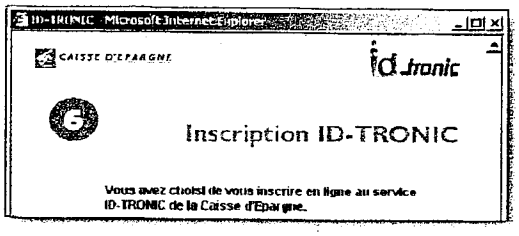
4 **Choisissez le bon site.**
On peut raisonnablement penser qu'un commerçant ayant pignon sur rue dispose de plus de moyens pour sécuriser son propre site. Et éviter ainsi que des pirates n'aboutissent facilement à la liste des numéros de carte de crédit des acheteurs en ligne. Préférez par conséquent les sites marchands d'enseignes reconnues.



5 **Préférez le paiement à des tiers de confiance.**
Dans certains cas, le paiement ne s'effectue pas directement au site marchand, mais à un tiers de confiance (banque, organisme de crédit), qui dispose de tous les moyens nécessaires pour sécuriser hautement tout son dispositif, les transactions comme le stockage des informations sensibles. Dans ce cas de figure, le site marchand ne disposera que d'un numéro d'agrément du tiers, assurant que le paiement a été effectué, et non du numéro de carte lui-même.

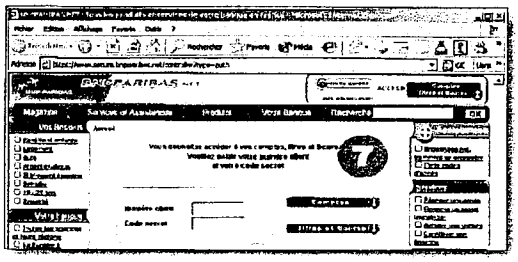


6 **Le paiement en ligne alternatif.**
Certaines banques proposent un autre moyen de paiement en ligne. L'internaute ne fournit pas en ligne son numéro de carte, mais un simple identifiant, complété d'un code transmis par SMS sur son téléphone mobile. Le risque de piratage est alors quasi nul.



7 **Surveillez vos relevés de compte.**
L'achat en ligne suppose une certaine surveillance de vos comptes bancaires. Pensez à vérifiez votre relevé mensuel à la recherche d'un débit ne correspondant à aucun achat connu.

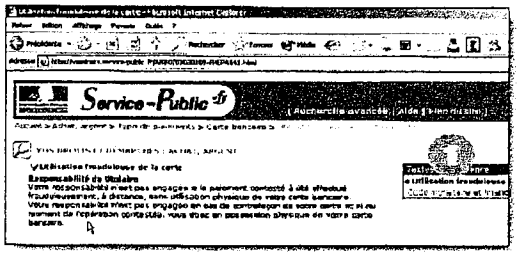
Pour une surveillance plus assidue, tirez parti des positions détaillées délivrées par certains distributeurs bancaires ou abonnez-vous à une gestion de compte bancaire en ligne.



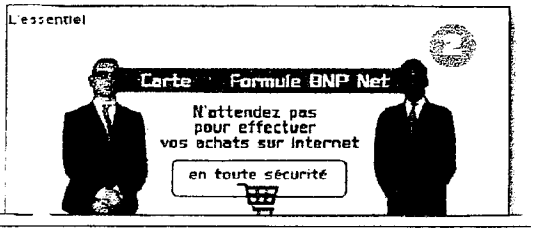
Assistance

Que faire en cas d'utilisation frauduleuse de votre carte ?

1 **Contestez le paiement auprès de votre banque**
Selon la loi « sécurité quotidienne » du 15 novembre 2001, la responsabilité du titulaire d'une carte bancaire n'est pas engagée si le paiement frauduleux a été effectué à distance, sans utilisation physique de la carte. Vous disposez d'un délai d'au moins 70 jours pour contester par écrit la transaction auprès de votre banque. Vous serez intégralement remboursé des sommes débitées frauduleusement, y compris celles qui ont précédé la découverte de la fraude et les éventuels frais y afférant. Ce remboursement doit avoir lieu dans un délai maximum de 30 jours à compter de la réception de la contestation.



2 **Les assurances anti-fraudes.**
Banques et assurances proposent des services, payants comme il se doit, pour couvrir les risques liés à l'achat sur Internet. Evaluez bien le contrat pour juger s'il présente un bénéfice notable par rapport à l'obligation légale imposée aux établissements bancaires.



DOCUMENT B

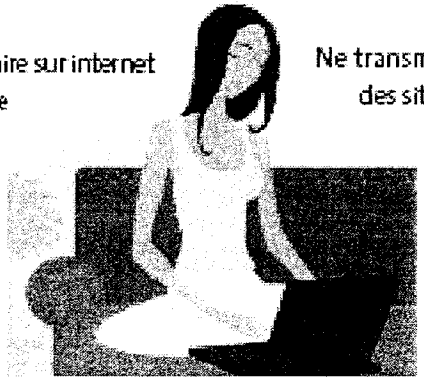
RÉSUMÉ D'UNE CONVERSATION AVEC UN CLIENT

Faites-vous confiance à l'achat en ligne et à la vente de produits sur internet ?

J'avoue que depuis que j'utilise ce procédé, je n'ai jamais eu de problème particulier et c'est tant mieux ! J'ai toujours une crainte mais je fais suffisamment confiance aux fournisseurs connus qui garantissent l'utilisation de leur système sécurisé en cryptant les données de la clientèle ; d'ailleurs avant de passer toute commande, il existe une rubrique qui nous indique toutes les informations nécessaires sur la sécurisation du système des moyens de paiement ; tout est expliqué pour rassurer le client.

DOCUMENT C

FEVAD ACHATS EN LIGNE COMMENT PAYER EN TOUTE SÉCURITÉ ?



L'utilisation de la carte bancaire sur internet n'est pas plus dangereuse que dans un magasin ou lors d'une commande passée par minitel ou par téléphone. Avant d'indiquer dans un formulaire en ligne votre numéro de carte bancaire et les 3 derniers chiffres figurant au dos de votre carte dans l'espace signature, ou plus rarement, à côté de son numéro au recto, vérifiez toujours que vous transmettez vos données bancaires de façon cryptée. Cela se traduit par une adresse de page (URL) commençant par « https » au lieu de « http » et parfois l'apparition d'un cadenas fermé en bas à gauche ou à droite de votre navigateur internet.

Ne transmettez pas vos données bancaires à des sites qui ne vous inspirent pas confiance ou qui ne donnent aucune indication sur la société ou aucun point de contact (adresse, téléphone, courriel).

Si votre numéro de carte bancaire fait l'objet d'un usage frauduleux sur internet, pas de panique ! Vous pourrez obtenir le remboursement des sommes débitées en adressant à votre banque une attestation écrite contestant le paiement.

Une telle démarche doit être effectuée dans les 70 jours suivant le débit. Dernière précaution, ne donnez à aucun moment votre code confidentiel à quatre chiffres qui ne sert que pour les paiements en magasin.

Le phishing, ou filoutage, constitue un grand danger pour l'internaute. C'est une technique par laquelle un escroc cherche à convaincre un internaute de lui communiquer ses données bancaires. Le fraudeur prend l'apparence, dans un courrier électronique et au travers d'un faux site internet, d'une banque ou d'un service connu pour vous demander vos informations confidentielles. La réponse à cette fraude est simple : ne tenez jamais compte du message reçu et supprimez-le !

À chaque forme d'achat son moyen de paiement

La carte bancaire est adaptée à un paiement au coup par coup. Elle est en revanche déconseillée pour des paiements à échéances régulières. Si vous souhaitez régler un abonnement de manière automatique et pouvoir interrompre le paiement à tout moment, il est préférable de recourir à une autorisation de prélèvement ou à un virement permanent. Le choix d'un tel mode de paiement peut toutefois retarder l'exécution du service.

Certains établissements financiers proposent des solutions spécifiques dédiées au paiement en ligne (e-Carte Bleue, ID Transac, paiement par des comptes externes, etc.).

Extrait du fichier informatisé sur un ratio de 700 clients dormants

Nom-adresse-téléphone	Date de la dernière commande	Nombre de points obtenus *	Observations
Mme JOFFRIN 4, rue Ste Catherine 59031 LILLE lydie.joffrin@wanadoo.fr	08/08/2006	4 000 points	
Mme BEAL 12, rue Gambetta 59000 LILLE catherine.beal@free.fr	05/10/2006	300 points	Réclamation pour retard de livraison
Mme BAZIN 36, rue Praire 59050 LILLE joelle.bazin@free.fr	15/09/2006	1 500 points	Absent la journée, marchandises à laisser au point relais

1. **Le client reçoit 10 points de fidélité par tranche de 15 €.**
2. **À partir de 4 000 points, 5 % sont ajoutés à toute offre de réduction.**
3. **À partir de 5 000 points, un catalogue de cadeaux est proposé.**
4. **Livraison garantie sous 15 jours.**

Offre de mai/juin

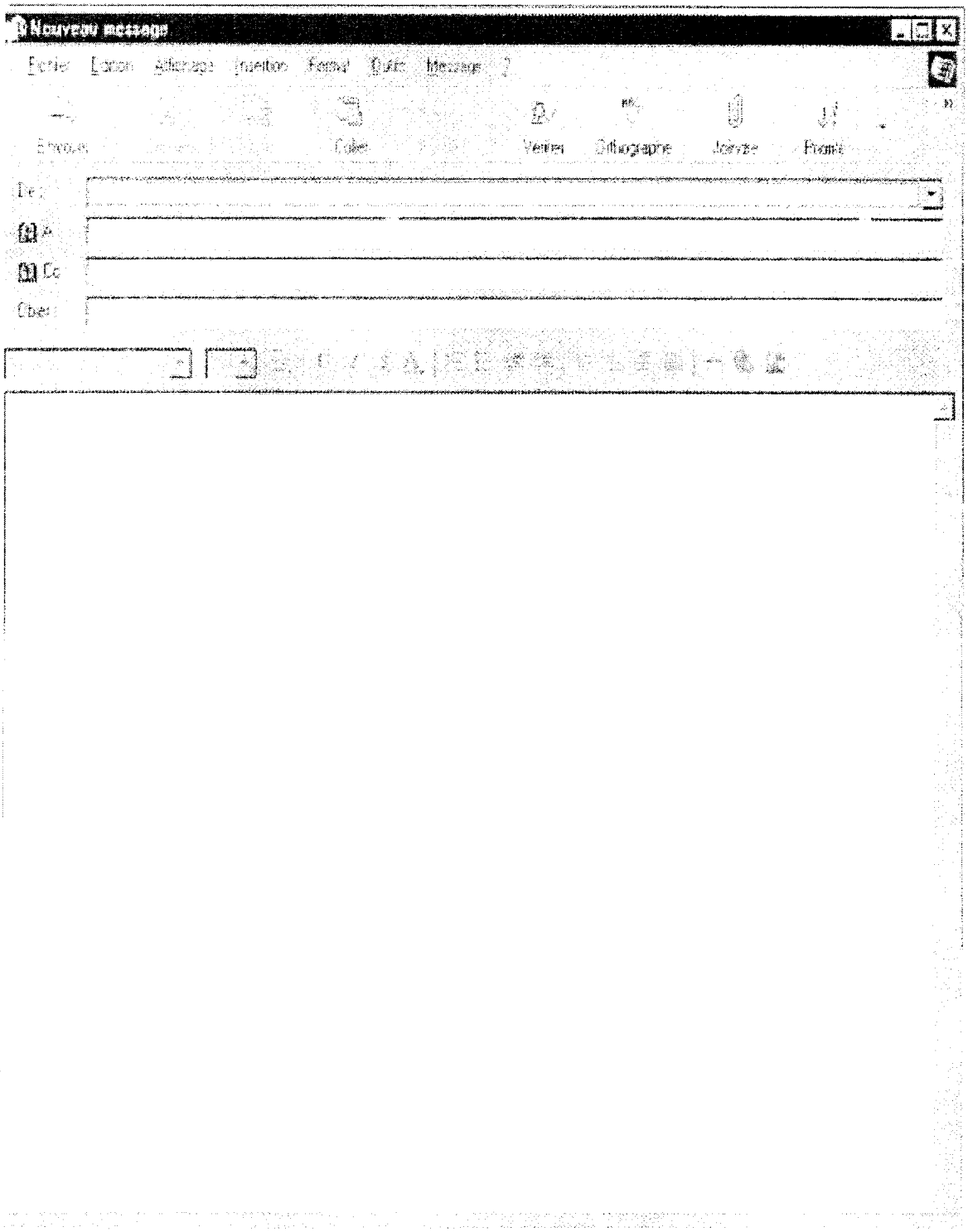
Dessous ravissants : Découvrez le Thermolactyl réputé pour sa chaleur, marié à la soie, au coton léger comme une caresse.

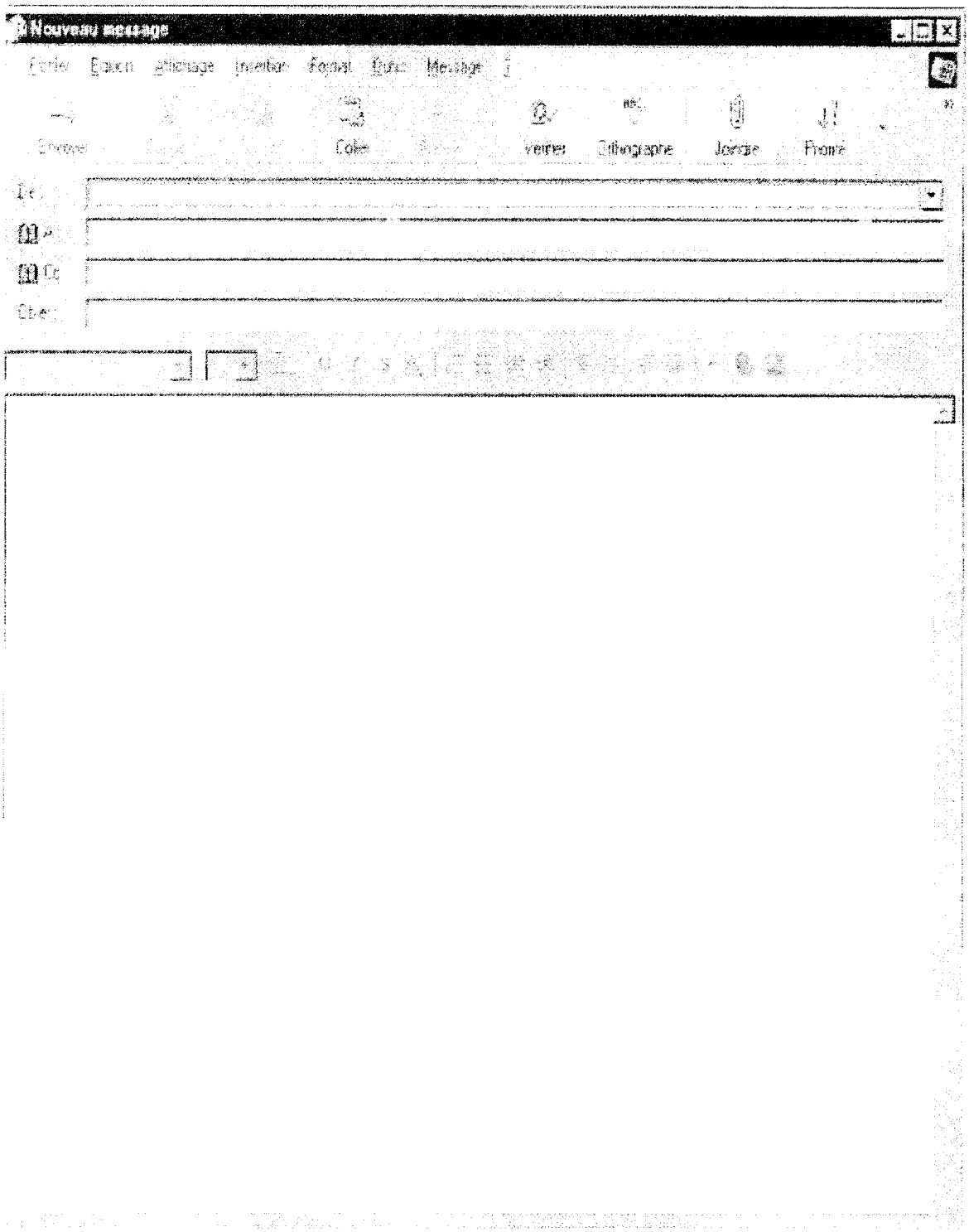
Ligne FEMME	**20 % de remise**
Ligne HOMME	**Trois pour deux**
Ligne ENFANT	**30 % de remise**

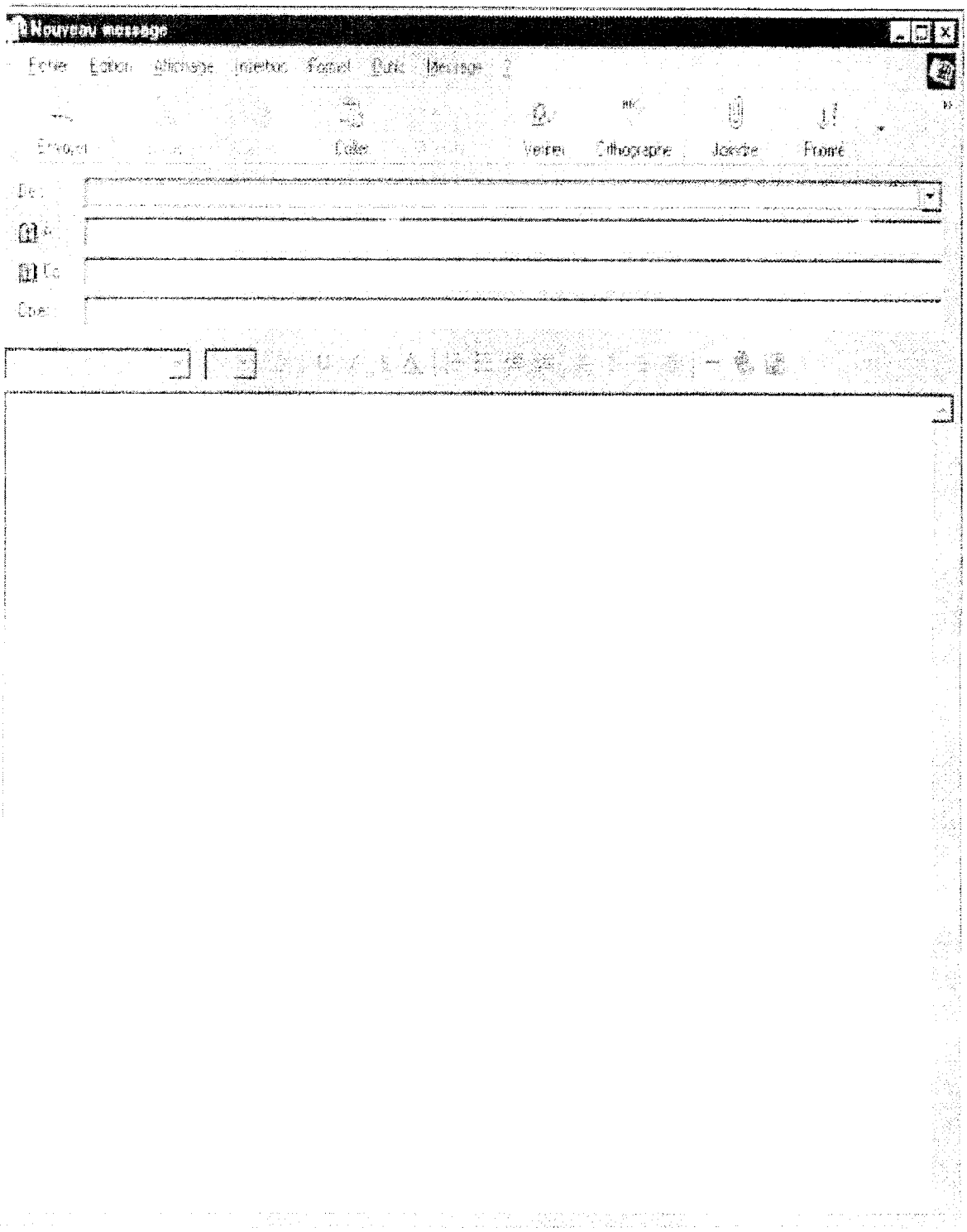
LA FOIRE AUX QUESTIONS

FOIRE AUX QUESTIONS	
QUESTIONS	REPONSES
Qu'est-ce que le paiement en ligne alternatif ?	
Que dois-je faire si je m'aperçois que ma carte de paiement a été utilisée ?	
Faut-il disposer d'une nouvelle version d'Internet explorer ?	
Est-ce que votre site est fiable ?	
Est-il préférable de ne pas payer directement sur le site ?	
Quels sont les risques si je règle en ligne ?	
Est-ce que je peux m'assurer contre les risques de fraude ?	
Comment les paiements sont-ils sécurisés ?	


BAMART
accueil


Nouveau message
Envoyer
Couper
Vérifier
Orthographe
Joindre
Priorité
De :
A :
Cc :
Objet :


Nouveau message
Envoyer
Coller
Vérifier
Orthographe
Joindre
Priorité
De :
A :
Cc :
Objet :


Nouveau message
Envoyer
Couper
Vérifier
Orthographe
Joindre
Priorité