Chapitre 15

Exercices

EXERCICE 1 – AUDIT D'UNE MESSAGERIE PROFESSIONNELLE DÉSORGANISÉE

1. Identifiez les dysfonctionnements constatés dans la gestion de la messagerie de M. Dubois.

L'audit de la messagerie de M. Dubois met en évidence cinq dysfonctionnements majeurs, qui contreviennent directement aux bonnes pratiques de gestion d'une messagerie professionnelle présentées dans le chapitre.

Dysfonctionnement n° 1 : l'accumulation de messages non lus (1 200 messages)
Ce volume colossal traduit une **absence totale de traitement régulier** des courriels entrants. La boîte de réception est utilisée comme une simple zone d'accumulation, sans tri ni traitement. Cette pratique pose plusieurs problèmes :

- des courriels importants risquent d'être noyés dans la masse et de **passer inaperçus** (information manquée, demande client sans réponse, échéance oubliée) ;
- la **fonction première de la boîte de réception** — alerter l'utilisateur sur les nouvelles communications — devient inopérante : avec 1 200 messages non lus, plus aucun signal ne se distingue ;
- le collaborateur risque la **perte de crédibilité professionnelle** auprès de ses interlocuteurs internes et externes, qui peuvent légitimement penser qu'il néglige ses échanges ;
- la **recherche d'information** devient extrêmement difficile, voire impossible.

Dysfonctionnement n° 2 : l'usage abusif de la fonction « Répondre à tous »
L'utilisation systématique de « Répondre à tous » sans discernement constitue une mauvaise pratique caractérisée. Elle entraîne :

- une **surcharge de la messagerie des collègues**, dont une partie reçoit des réponses qui ne les concernent pas ;
- un phénomène d'**« infobésité »** qui dégrade la productivité collective ;
- un **risque de divulgation involontaire** d'informations à des personnes qui n'ont pas à les connaître ;
- une **perte de pertinence des échanges** : à force de recevoir des messages sans intérêt, les destinataires finissent par ne plus lire attentivement les courriels collectifs.

Dysfonctionnement n° 3 : la conservation des pièces jointes volumineuses dans la boîte
Le fait de ne pas archiver les pièces jointes en dehors de la messagerie pose plusieurs difficultés :

- une **saturation rapide de l'espace de stockage** alloué à la boîte aux lettres, qui peut conduire au blocage de la réception de nouveaux messages ;
- un **ralentissement des performances** du logiciel de messagerie (synchronisation lente, recherche difficile) ;
- une **mauvaise traçabilité documentaire** : les documents importants ne sont pas rangés dans un système structuré (serveur partagé, GED) et restent inaccessibles aux collègues ;
- une **perte potentielle en cas d'incident technique** sur la messagerie.

Dysfonctionnement n° 4 : l'impression de courriels personnels laissés en salle commune

Cette pratique cumule plusieurs manquements :

- une **atteinte à la confidentialité** : laisser des courriels imprimés dans un espace partagé expose leur contenu à toute personne de passage ;
- un **manquement aux règles de protection des données personnelles** (RGPD), notamment si les courriels contiennent des informations sur des collègues, des clients ou des fournisseurs ;
- une **dégradation de l'image professionnelle** du collaborateur, qui ne distingue pas la sphère privée de la sphère professionnelle ;
- un **gaspillage** contraire aux principes d'écologie numérique évoqués dans le cours (impressions inutiles).

Dysfonctionnement n° 5 : l'absence totale de filtres ou de règles de classement

L'absence d'organisation systémique de la messagerie traduit une mauvaise maîtrise de l'outil :

- aucun **dossier thématique** n'est créé pour structurer le classement (par projet, par client, par mission) ;
- aucune **règle de filtrage automatique** n'est paramétrée pour orienter les messages selon leur expéditeur ou leur objet ;
- aucune **priorisation** n'est mise en place pour signaler les messages stratégiques ;
- le travail de tri repose entièrement sur la mémoire et la réactivité du collaborateur, qui ne peut, faute d'organisation, traiter correctement le volume reçu.

Synthèse

Ces cinq dysfonctionnements forment un **système cohérent de mauvaises pratiques** : l'absence d'organisation engendre l'accumulation, l'accumulation rend impossible le tri, et l'absence de tri amplifie encore le désordre. M. Dubois se trouve dans une situation classique d'**infobésité aggravée**, où la messagerie est devenue un outil de désorganisation plutôt qu'un outil de productivité.

2. Proposez un plan d'action détaillé pour améliorer l'organisation et l'utilisation de sa messagerie.

Pour remédier aux dysfonctionnements identifiés, un plan d'action structuré en trois phases est proposé : une phase de **remise à plat immédiate** de la messagerie, une phase de **structuration durable**, et une phase **d'ancrage des bonnes pratiques**.

Phase 1 – Remise à plat immédiate (1 à 2 jours)

L'objectif est de rendre la boîte de réception à nouveau exploitable.

1. **Vidage progressif de la boîte de réception** : traiter les 1 200 messages non lus en plusieurs séances de travail courtes (1 heure par jour pendant une semaine), en appliquant la règle des « 4 actions » à chaque courriel :
    - **traiter** s'il appelle une réponse ou une action immédiate ;
    - **classer** dans un dossier dédié s'il doit être conservé ;
    - **transférer** au bon interlocuteur s'il ne relève pas de sa compétence ;
    - **supprimer** s'il est obsolète, redondant ou sans valeur.
2. **Externalisation des pièces jointes volumineuses** : extraire les documents conservés vers un **serveur partagé** ou un système de gestion documentaire (GED), en respectant les règles de nommage et de classement de l'entreprise. Cette opération libère l'espace de stockage de la messagerie et améliore la traçabilité documentaire.
3. **Collecte et destruction sécurisée des impressions papier** : récupérer les courriels imprimés laissés en salle commune et les éliminer via les circuits de destruction sécurisée (broyeur), notamment pour ceux contenant des données personnelles.

Phase 2 – Structuration durable (1 semaine)

L'objectif est de mettre en place une architecture de messagerie durable.

1. **Création d'une arborescence de dossiers adaptée à l'activité du collaborateur :**
    - dossiers **par projet** (Projet ALPHA, Projet BÊTA…) ;
    - dossiers **par client** (Client Dupont SA, Client Martin SARL…) ;
    - dossiers **par mission ou service** (Comptabilité fournisseurs, Reporting RH…) ;
    - dossier « **À traiter** » pour les courriels en attente d'action ;
    - dossier « **Archives** » pour les éléments conservés à long terme.
2. **Paramétrage de règles automatiques :**
    - filtrage par expéditeur (les courriels d'un client donné sont automatiquement classés dans son dossier) ;
    - filtrage par objet (les messages contenant « Facture » sont dirigés vers le dossier comptabilité) ;
    - marquage automatique des messages urgents en provenance de la hiérarchie ;
    - suppression automatique des newsletters non lues après 30 jours.
3. **Mise à jour du carnet d'adresses :**
    - création de **listes de diffusion** pour les groupes d'interlocuteurs fréquents (équipe projet, service comptable, fournisseurs récurrents) ;
    - suppression des contacts obsolètes ;
    - synchronisation avec le téléphone professionnel.
4. **Configuration de la signature électronique** complète (nom, fonction, coordonnées, mentions légales éventuelles) pour véhiculer une image professionnelle cohérente.

Phase 3 – Ancrage des bonnes pratiques (à pérenniser)

L'objectif est de transformer ces aménagements en habitudes durables.

1. **Routine quotidienne de traitement** : prévoir deux à trois plages dédiées au traitement de la messagerie (matin, milieu de journée, fin d'après-midi) plutôt qu'une consultation continue source de dispersion.
2. **Règles d'usage à respecter systématiquement** :
    - rédiger un **objet précis** pour chaque courriel envoyé ;
    - limiter l'usage de « Répondre à tous » aux cas où **tous** les destinataires sont réellement concernés ;
    - **annoncer les pièces jointes** dans le corps du message et vérifier leur présence avant l'envoi ;
    - répondre dans un **délai de 24 à 48 heures** lorsque cela est attendu.
3. **Activation systématique du message d'absence** lors des congés, déplacements ou arrêts, en mentionnant la date de retour et un contact de remplacement.
4. **Audit mensuel de la messagerie** : consacrer 30 minutes par mois à vérifier l'efficacité des filtres, supprimer les dossiers obsolètes, mettre à jour le carnet d'adresses

3. Analysez les risques professionnels et organisationnels liés à ces mauvaises pratiques.

Les dysfonctionnements observés ne sont pas de simples maladresses : ils exposent le collaborateur et l'organisation à des risques significatifs, qui peuvent se traduire par des conséquences professionnelles, économiques et juridiques.

Risques professionnels pour le collaborateur

Sur le plan **individuel**, M. Dubois s'expose tout d'abord à une **perte de productivité** importante. Le temps consacré à rechercher un courriel dans une boîte saturée, à traiter en urgence un message tardivement repéré ou à reconstituer un échange perdu pèse lourdement sur l'efficacité quotidienne. À titre d'illustration, des études managériales estiment qu'un cadre passe en moyenne **2 à 3 heures par jour** sur sa messagerie ; lorsque celle-ci est désorganisée, ce temps est largement improductif.

La désorganisation entraîne également un **risque d'oubli d'échéances** : factures non payées dans les délais, demandes clients sans suite, convocations manquées. Chacun de ces incidents peut être imputé personnellement au collaborateur et alimenter une appréciation négative de son professionnalisme.

À terme, ces dysfonctionnements affectent la **crédibilité professionnelle** du collaborateur. Ses collègues, sa hiérarchie et ses interlocuteurs externes peuvent percevoir négativement sa difficulté à répondre, sa désorganisation visible (impressions laissées en salle commune) et la qualité variable de ses échanges. Le risque ultime est celui de **sanctions professionnelles**, voire d'une remise en cause du contrat de travail en cas de manquements répétés et avérés.

Risques organisationnels pour l'entreprise

Au-delà du collaborateur, l'entreprise subit elle aussi les conséquences de ces mauvaises pratiques.

Le premier risque est **financier**. Une demande client manquée peut entraîner la perte d'un contrat ; un retard de paiement non détecté peut générer des pénalités ; une opportunité commerciale ignorée peut profiter à un concurrent. La désorganisation d'une messagerie individuelle peut ainsi entraîner des **répercussions directes sur le chiffre d'affaires de l'entreprise**.

Le deuxième risque est **opérationnel**. Lorsque les pièces jointes restent enfermées dans une messagerie individuelle plutôt que d'être archivées sur un serveur partagé, l'information n'est pas accessible à l'équipe. En cas d'absence du collaborateur, ses collègues ne peuvent reprendre ses dossiers. La continuité d'activité est compromise.

Le troisième risque, sans doute le plus grave, est **juridique et lié à la confidentialité**. Les impressions de courriels laissées en salle commune, combinées à l'absence de tri des messages, exposent l'entreprise à plusieurs manquements :

- non-respect du **RGPD** : les données à caractère personnel (collègues, clients, fournisseurs) doivent être protégées contre tout accès non autorisé. Des courriels imprimés et abandonnés constituent une faute caractérisée susceptible d'engager la responsabilité de l'entreprise vis-à-vis de la CNIL ;

- **divulgation d'informations confidentielles** : un courriel imprimé peut contenir des informations stratégiques, financières ou commerciales que des tiers (visiteurs, prestataires, autres salariés) ne devraient pas connaître ;

- **risque de réputation** : la diffusion non maîtrisée d'informations peut altérer l'image de l'entreprise auprès de ses partenaires.

Le quatrième risque concerne la **sécurité informatique**. Une messagerie négligée, dans laquelle les messages s'accumulent sans tri, augmente la probabilité qu'un courriel frauduleux (phishing, virus en pièce jointe) passe inaperçu et soit ouvert par mégarde. La sécurité de l'ensemble du système d'information de l'entreprise peut alors être compromise (vol de données, rançongiciel, paralysie du réseau).

Enfin, sur le plan **managérial**, ces pratiques peuvent générer des **tensions au sein de l'équipe** : collègues lassés par les « Répondre à tous » abusifs, hiérarchie agacée par les retards de traitement, ressentiment lié à la nécessité de pallier les manquements du collaborateur défaillant. Le climat de travail se dégrade et la dynamique collective en pâtit.

EXERCICE 2 – RÉDIGER UN COURRIEL DE CANDIDATURE A UN STAGE

1. Quels éléments doivent impérativement figurer dans l'objet du courriel ?

L'objet du courriel constitue le **premier point de contact** entre le candidat et le recruteur. Il est lu en quelques fractions de seconde et conditionne souvent la décision même d'ouvrir le message. Un objet vague, mal formulé ou absent expose le courriel à plusieurs risques : non-lecture, archivage automatique par les filtres antispam, ou simple oubli dans une boîte de réception surchargée. Dans le cadre d'une candidature, où la concurrence entre profils est forte, ce risque est rédhibitoire.

L'objet d'un courriel de candidature doit donc être **précis, concis et immédiatement informatif**. Il doit permettre au recruteur d'identifier en un coup d'œil quatre éléments clés :

1. La nature de la démarche : « Candidature »

Le mot « Candidature » doit figurer explicitement dans l'objet. Il signale au destinataire qu'il s'agit d'une démarche spontanée ou d'une réponse à une offre, et permet au service ressources humaines de classer immédiatement le message dans le bon flux de traitement.

2. Le type de poste recherché : « stage »

Préciser qu'il s'agit d'un stage (et non d'un emploi en CDI, d'une alternance ou d'un job d'été) oriente immédiatement le destinataire vers le bon interlocuteur interne (responsable de la formation, tuteur potentiel, service RH dédié aux stagiaires).

3. Le domaine ou la fonction : « comptabilité »

Le domaine professionnel doit être mentionné, particulièrement dans un cabinet qui peut proposer des stages dans plusieurs spécialités (comptabilité, audit, conseil, social, juridique). Cette précision démontre également une candidature ciblée et non générique.

4. La période ou la durée : « Avril à juin 2027 »

L'indication de la période permet au recruteur de vérifier immédiatement la compatibilité de la candidature avec ses besoins (effectifs, charge d'activité, plan de charge des tuteurs). Une candidature pour une période où le cabinet n'accueille pas de stagiaires sera écartée d'office, ce qui évite des échanges inutiles.

Élément complémentaire optionnel : la formation du candidat

Selon la place disponible, il peut être pertinent de mentionner le diplôme préparé (« DCG 2e année »), notamment si le candidat répond à une offre ne précisant pas le niveau attendu. Cette information rassure le recruteur sur le profil et évite les candidatures inappropriées.

Exemples d'objets adaptés

- Objet : **Candidature stage en comptabilité – DCG 2e année – Avril à juin 2027**
- Objet : **Candidature à un stage de 8 semaines en comptabilité – Avril 2027**
- Objet : **Candidature stage comptabilité – Offre cabinet ComptaExpert – Printemps 2027**

Exemples d'objets à éviter

- « Candidature » (trop vague, ne distingue pas le type de candidature)
- « Stage » (n'indique ni le domaine ni la période)
- « URGENT – Candidature » (le mot URGENT est déplacé dans une candidature et peut alerter les filtres antispam)
- « Bonjour » ou « Demande » (objets vides de sens)
- Absence totale d'objet (le courriel risque de ne jamais être ouvert)

L'objet doit ainsi répondre à un principe simple : **un destinataire qui le lit doit pouvoir, sans ouvrir le message, savoir exactement de quoi il s'agit**.

2. **Rédigez le corps du message de candidature (3 à 4 paragraphes maximum).**

De : julien.martin@etu-tarbes.fr

À : recrutement@comptaexpert.fr

Objet : Candidature stage en comptabilité – DCG 2e année – Avril à juin 2027

Madame, Monsieur,

Actuellement étudiant en deuxième année de Diplôme de Comptabilité et de Gestion au lycée Marie Curie de Tarbes, je suis à la recherche d'un stage obligatoire de huit semaines, du 6 avril au 29 mai 2027. L'offre que vous avez publiée sur le site internet du cabinet ComptaExpert a retenu toute mon attention et correspond précisément aux compétences que je souhaite développer à ce stade de ma formation.

Ma formation m'a permis d'acquérir des bases solides en comptabilité générale, comptabilité approfondie et droit fiscal, ainsi qu'une première pratique du logiciel Sage. Mon expérience de trésorier de l'association étudiante de mon établissement m'a par ailleurs amené à pratiquer le rapprochement bancaire mensuel et le suivi des règlements, opérations directement liées aux missions que vous proposez. La diversité des dossiers traités au sein de votre cabinet, reconnu pour la qualité de son accompagnement des PME locales, représente pour moi un cadre idéal pour consolider ces acquis et découvrir le métier d'expert-comptable dans son environnement réel.

Vous trouverez en pièces jointes mon curriculum vitæ ainsi que ma lettre de motivation, qui détaillent mon parcours et précisent les raisons qui motivent ma démarche auprès de votre

cabinet. Je me tiens à votre entière disposition pour un entretien à la date qui vous conviendra.

Je vous remercie par avance de l'attention que vous voudrez bien porter à ma candidature.

Justification des choix rédactionnels

Ce courriel respecte l'ensemble des exigences présentées dans le chapitre.

Sur la **structure**, le message respecte la règle des trois étapes :

- **L'introduction** (premier paragraphe) présente le candidat, l'objet de la démarche, la période visée et la source de l'annonce. Le recruteur dispose en quelques lignes des informations essentielles pour situer la candidature.
- **Le développement** (deuxième paragraphe) valorise les compétences techniques (comptabilité, droit fiscal, Sage) et les expériences pratiques (trésorerie associative) en lien direct avec les missions du stage. Une phrase montre que le candidat connaît le cabinet et a réfléchi à son adéquation avec ses propres attentes.
- **La conclusion** (troisième paragraphe) annonce les pièces jointes et propose une suite à la démarche (entretien). Le quatrième paragraphe court constitue un remerciement courtois.

Sur la **forme**, plusieurs principes ont été respectés :

- la **formule d'appel** « Madame, Monsieur, » est neutre et adaptée lorsque le destinataire précis n'est pas identifié ;
- le **vocabulaire** est précis et professionnel, sans abréviation ni familiarité ;
- les **phrases sont courtes** et structurées, conformes aux exigences d'un écrit professionnel ;
- les **pièces jointes sont annoncées** explicitement dans le corps du message, conformément aux bonnes pratiques rappelées dans le cours ;
- la **longueur** est calibrée : suffisamment développée pour convaincre, suffisamment concise pour respecter le format courriel.

3. Proposez deux noms explicites pour vos pièces jointes (CV et lettre).

Le nommage des pièces jointes est un point souvent négligé qui produit pourtant des effets concrets sur la qualité perçue de la candidature. Un fichier intitulé « CV.pdf » ou « document1.docx » est immédiatement perdu dans le dossier du recruteur, qui reçoit potentiellement plusieurs dizaines de candidatures par semaine, toutes accompagnées de fichiers homonymes. Un nom de fichier précis présente trois avantages :

1. **Identification immédiate** par le recruteur, qui peut classer le document sans l'ouvrir ;
2. **Recherche facilitée** par mots-clés au sein des dossiers de candidatures ;
3. **Image professionnelle** valorisée : le candidat démontre sa maîtrise des codes de la communication numérique.

Les règles de nommage à respecter sont les suivantes : utiliser un format clair, séparer les éléments par des underscores ou des tirets, éviter les espaces (qui peuvent poser des problèmes lors du téléchargement) et privilégier le format **PDF** (format universel, non modifiable, lecture identique sur tous les supports).

Propositions de nommage

Pièce jointe	**Nom proposé**
Curriculum vitæ	**CV_MARTIN_Julien_DCG2_2027.pdf**
Lettre de motivation	**LM_MARTIN_Julien_Stage_ComptaExpert.pdf**

Variantes possibles, également correctes

- **CV_Julien_MARTIN.pdf** et **Lettre_motivation_Julien_MARTIN.pdf** (version plus simple)
- **Martin_Julien_CV_Stage_Compta_2027.pdf** et **Martin_Julien_LM_Stage_Compta_2027.pdf** (nom du candidat en premier, utile pour le classement alphabétique par le recruteur)

Éléments à proscrire dans les noms de fichiers

- noms génériques (CV.pdf, lettre.docx, document1.pdf) ;
- mention de versions (CV_final_v3.pdf, lettre_definitive_corrigee.pdf), qui révèlent un travail non finalisé ;
- accents et caractères spéciaux (CVéditeur.pdf), qui peuvent poser des problèmes de compatibilité ;
- espaces dans le nom de fichier (CV Julien Martin.pdf), qui peuvent provoquer des erreurs d'affichage selon les systèmes d'exploitation.

4. Quelle formule de politesse est adaptée à ce type de courriel ?

Le choix de la formule de politesse constitue un équilibre subtil. Le candidat doit témoigner du **respect dû au destinataire** d'une candidature, sans pour autant adopter un registre trop solennel qui serait inadapté au format du courriel.

Le cours distingue clairement les usages : le courriel privilégie des formules **brèves et neutres**, là où la lettre papier admet des formules plus longues et plus protocolaires. Transposer la formule conventionnelle de la lettre (« Veuillez agréer, Madame, Monsieur, l'expression de mes salutations distinguées ») dans un courriel produit un effet maladroit, voire pompeux, qui dessert le candidat.

À l'inverse, des formules trop familières (« Cdlt », « Bises », « À+ ») ou trop personnelles sont à proscrire absolument dans un cadre professionnel, *a fortiori* lorsqu'il s'agit d'une candidature à un poste.

Formules de politesse recommandées pour un courriel de candidature

Formule	Niveau de formalité	Contexte d'usage
Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations respectueuses.	Soutenu	Candidature formelle, premier contact avec un cabinet ou une entreprise de renom
Avec mes salutations distinguées,	Soutenu	Candidature à un poste exigeant un haut niveau de formalisme
Bien respectueusement,	Soutenu mais bref	Bon compromis entre formalité et concision adaptée au courriel
Cordialement,	Standard	Formule passe-partout, acceptable mais moins valorisante pour une candidature

Formule recommandée pour le courriel rédigé en question 2

La formule la mieux adaptée à ce courriel de candidature est :

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations respectueuses.

Julien MARTIN Étudiant en 2e année de DCG 06 11 22 33 44 julien.martin@etu-tarbes.fr

Cette formule présente plusieurs qualités :

- elle **témoigne du respect** dû à un recruteur potentiel, en mobilisant le verbe « agréer » qui marque la déférence ;
- elle reste **suffisamment brève** pour un format courriel, là où une formule de lettre « complète » serait excessive ;
- l'adjectif « **respectueuses** » est plus approprié à une candidature que « distinguées », car il marque la position du candidat sollicitant le destinataire ;
- elle est **systématiquement accompagnée d'une signature complète** : nom et prénom (en majuscules ou italiques selon l'usage), statut, coordonnées téléphoniques et électroniques. Cette signature constitue la carte de visite du candidat et facilite la prise de contact ultérieure par le recruteur.

Formules à éviter dans une candidature

- « Bonne journée » (trop familier, ne marque aucun respect particulier) ;
- « Merci d'avance » seul (sans formule de politesse, donne une impression d'inachevé) ;
- « Cdlt » ou « Bien à vous » (le premier est une abréviation à proscrire, le second est trop informel pour un premier contact) ;

- « Sentiments dévoués » ou « Très humblement vôtre » (formules désuètes, voire ironiques aujourd'hui).

La règle d'or à retenir : **dans un courriel de candidature, la formule de politesse doit traduire le respect du destinataire tout en restant adaptée au format numérique du courriel — ni trop courte, ni trop solennelle**

EXERCICE 3 – IDENTIFIER ET PREVENIR UNE TENTATIVE DE PHISHING

1. Relevez au moins cinq indices montrant qu'il s'agit d'une tentative de phishing.

Le message reçu présente l'ensemble des caractéristiques typiques d'une tentative d'hameçonnage. Une analyse méthodique permet d'identifier au moins **sept indices convergents**, dont l'accumulation ne laisse aucun doute sur la nature frauduleuse du courriel.

Indice n° 1 : une adresse d'expéditeur suspecte

L'adresse securite@banquex.fr peut sembler crédible au premier regard, mais elle doit faire l'objet d'une analyse rigoureuse. Plusieurs éléments éveillent la méfiance :

- les véritables messages de sécurité d'une banque émanent généralement d'une **adresse précise et identifiable** du domaine officiel, souvent associée à une plateforme dédiée (par exemple : securite-clients@banquex.com avec une signature numérique vérifiable) ;
- le terme générique **« securite »** sans personnalisation ni référence à un service identifié est inhabituel pour une communication réelle ;
- il faudrait surtout vérifier si le **domaine banquex.fr** correspond bien au domaine officiel de la banque. Les fraudeurs utilisent fréquemment des domaines très proches (banquex.fr au lieu de banquex.com, banque-x.fr, banquex-securite.fr) pour tromper l'œil du lecteur non averti.

Le simple fait que l'adresse paraisse plausible ne constitue jamais une garantie : l'**usurpation d'adresse expéditrice** (technique appelée *spoofing*) est l'un des premiers outils du fraudeur.

Indice n° 2 : un objet alarmiste et créateur d'urgence

L'objet **« URGENT – Mise à jour obligatoire de votre compte »** cumule plusieurs marqueurs caractéristiques du phishing :

- l'emploi du mot **« URGENT » en majuscules** vise à provoquer une réaction émotionnelle (panique, précipitation) qui empêche le destinataire de prendre le temps d'analyser le message ;

- le terme **« obligatoire »** mobilise le levier de l'autorité : il suggère que le destinataire n'a pas le choix et doit obéir ;
- une banque sérieuse ne communique jamais en ces termes dans un objet de courriel. Les communications officielles emploient un registre **neutre et professionnel** (« Information importante concernant votre compte », « Évolution de nos conditions générales »).

Cette combinaison urgence + obligation est l'**empreinte typique** du phishing : elle court-circuite la réflexion du destinataire.

Indice n° 3 : une formule d'appel impersonnelle

La formule **« Cher client »** est extrêmement révélatrice. Une banque légitime, qui dispose des données nominatives de ses clients, personnalise systématiquement ses communications :

- « Madame Dupont, »
- « Monsieur Martin, »
- ou, à défaut, « Madame, Monsieur, » accompagné d'un numéro de référence client.

L'emploi d'une formule générique **« Cher client »** signale qu'il s'agit d'un **envoi de masse** indistinct, expédié à des milliers d'adresses sans aucune connaissance des destinataires réels. C'est la signature classique d'une campagne de phishing.

Indice n° 4 : une menace de blocage et un délai très court

La phrase **« Votre compte sera suspendu sous 24h si vous ne confirmez pas vos identifiants »** combine deux ressorts psychologiques manipulatoires :

- la **menace explicite** (suspension du compte), qui active la crainte de perdre l'accès à ses ressources financières ;
- le **délai très court** (24 heures), qui empêche toute vérification posée auprès de la banque ou auprès d'un collègue.

Les vraies communications bancaires laissent toujours au client le temps de réagir, proposent **plusieurs canaux de contact** (téléphone, agence, espace client sécurisé) et ne formulent jamais d'ultimatum aussi brutal. Un délai de 24 heures pour une opération critique est en réalité totalement irréaliste pour un service bancaire qui fonctionne en jours ouvrés.

Indice n° 5 : une demande inhabituelle d'identifiants

La sollicitation de **confirmation des identifiants** est l'indice le plus probant : **aucune banque, aucune administration, aucun fournisseur sérieux ne demande jamais par courriel la transmission ou la confirmation d'identifiants, de mots de passe ou de codes confidentiels**. Cette règle, rappelée dans le cours, ne souffre aucune exception.

Toute communication officielle, lorsqu'elle nécessite une intervention du client, l'invite à se connecter **directement** depuis son espace personnel sécurisé via l'application ou le site officiel, jamais en cliquant sur un lien reçu par courriel.

Indice n° 6 : un lien hypertexte suspect

Le lien **www.banquex-verification.com** présente plusieurs anomalies :

- il utilise un **domaine différent** du domaine officiel banquex.fr mentionné dans l'adresse expéditrice. Cette incohérence entre le domaine de l'expéditeur et le domaine du lien est un signal d'alarme majeur ;
- le mot **« verification »** dans l'URL est un terme employé par les fraudeurs pour donner une apparence de légitimité technique ;
- l'**extension .com** au lieu de .fr peut trahir une domiciliation à l'étranger, hors de la juridiction française ;
- en survolant le lien sans cliquer (sur ordinateur), il est probable que l'URL réelle affichée en bas de l'écran soit encore différente, masquant la véritable destination frauduleuse.

Indice n° 7 : l'absence d'éléments d'authentification habituels

Une communication bancaire officielle comporte généralement :

- la **signature complète** d'un service identifié, avec coordonnées et mentions légales ;
- un **rappel des coordonnées du client** (numéro de référence, agence) attestant que la banque connaît effectivement la personne ;
- des **mentions de sécurité** (« Ne communiquez jamais vos identifiants par courriel ») ;
- éventuellement un **logo certifié** et des liens vers les canaux officiels.

Le message reçu se contente d'une signature vague (« L'équipe Sécurité BanqueX ») sans aucun élément vérifiable d'authentification.

2. Rédigez un courriel d'alerte interne à destination de vos collègues expliquant les risques et la conduite à tenir.

De : stagiaire.securite@banquex.fr

À : ensemble.collaborateurs@banquex.fr

Cc : responsable.informatique@banquex.fr

Objet : Alerte – Tentative de phishing en cours : conduite à tenir

Chers collègues,

Le service informatique a identifié au cours des dernières heures la circulation d'un courriel frauduleux usurpant l'identité de notre établissement. Ce message, intitulé « **URGENT – Mise à jour obligatoire de votre compte** », invite les destinataires à confirmer leurs identifiants en cliquant sur un lien externe. **Il s'agit d'une tentative de phishing** : ce courriel ne provient pas de la banque.

Identifier ce type de message

Plusieurs indices permettent de reconnaître une tentative de phishing :

- une adresse expéditrice ressemblant à une adresse officielle mais comportant une légère variation (domaine, extension) ;
- un objet alarmiste créant un sentiment d'urgence (« URGENT », « obligatoire », menace de suspension) ;
- une formule d'appel impersonnelle (« Cher client » au lieu d'un nom précis) ;
- une demande de transmission ou de confirmation d'identifiants, de mots de passe ou de coordonnées bancaires ;
- un lien hypertexte renvoyant vers un site dont l'adresse ne correspond pas au domaine officiel de l'établissement.

Pour mémoire, **aucune banque, aucune administration ne demande jamais par courriel la communication d'identifiants ou de mots de passe.**

Conduite à tenir

Si vous recevez un message présentant ces caractéristiques, ou si vous avez un doute sur un courriel reçu :

1. **Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe.**
2. **Ne répondez pas au message** et ne transmettez aucune information personnelle.
3. **Signalez le courriel** à l'adresse signalement.phishing@banquex.fr en le transférant avec son en-tête complet (option « Transférer en tant que pièce jointe » dans Outlook).
4. **Supprimez ensuite le message** de votre boîte de réception et de votre dossier « Éléments supprimés ».

5. En cas de doute, **contactez directement le service informatique** au poste 1234 avant toute action.

Si vous avez malencontreusement cliqué sur le lien ou transmis des informations, **contactez immédiatement le service informatique** : des mesures de sécurité (changement de mots de passe, blocage de comptes) seront mises en œuvre sans délai.

Sensibilisation des clients

Nous vous rappelons par ailleurs qu'en tant que collaborateurs de la banque, nous sommes en première ligne pour sensibiliser nos clients à ces pratiques frauduleuses. N'hésitez pas à les inviter à la vigilance lors de vos prochains échanges et à leur rappeler les bons réflexes (vérification de l'expéditeur, connexion uniquement depuis le site officiel, signalement de toute communication suspecte au 3000).

Je vous remercie de l'attention que vous porterez à ce message et de votre vigilance.

Bien cordialement,

Julien MARTIN Stagiaire – Service Sécurité informatique Poste : 5678
julien.martin@banquex.fr

3. Proposez trois mesures de prévention que la banque pourrait mettre en place pour renforcer la vigilance des salariés et des clients.

La sécurité face au phishing ne peut reposer sur la seule vigilance individuelle des collaborateurs et des clients. Elle suppose une **politique de prévention structurée**, articulée autour de mesures techniques, humaines et organisationnelles. Trois axes complémentaires peuvent être proposés à la direction de la banque.

Mesure n° 1 – Mettre en place un programme de formation et de sensibilisation continue

Il s'agit d'agir sur le **facteur humain**, identifié dans toutes les études en cybersécurité comme le maillon le plus exposé. La technique la plus avancée des pirates exploite en premier lieu les comportements humains : précipitation, confiance excessive, méconnaissance des signaux d'alerte.

Le programme proposé pourrait comporter :

- **Une formation initiale obligatoire** à l'embauche de tout nouveau collaborateur, couvrant l'identification des courriels frauduleux, les conduites à tenir et les procédures de signalement. Cette formation peut prendre la forme d'un module e-learning d'environ une heure, suivi d'un quiz de validation.
- **Une formation continue annuelle** pour l'ensemble du personnel, intégrée au plan de formation. Le contenu doit être actualisé chaque année en fonction des nouvelles techniques d'attaque observées sur le marché. Une attention particulière doit être

portée aux services les plus exposés : accueil clients, gestionnaires de comptes, service informatique.

- **Des campagnes de phishing simulé** organisées par la cellule sécurité ou un prestataire spécialisé. Le principe consiste à envoyer aux collaborateurs de faux courriels de phishing inoffensifs ; ceux qui cliquent sont immédiatement redirigés vers une page pédagogique expliquant les indices qu'ils auraient dû identifier. Ces simulations, à la fois ludiques et révélatrices, sont particulièrement efficaces pour ancrer les bons réflexes.
- **Une communication régulière** sur les tentatives détectées : courriels d'alerte (comme celui rédigé en question 2), affichage dans les espaces communs, rubriques dédiées dans la newsletter interne. La répétition est la clé de l'ancrage durable des comportements de vigilance.

Mesure n° 2 – Déployer des dispositifs techniques de filtrage et d'authentification

La prévention humaine doit s'accompagner d'une **protection technique robuste**, capable de bloquer en amont la majorité des courriels frauduleux avant qu'ils n'atteignent les destinataires.

Plusieurs dispositifs peuvent être mobilisés :

- **Un système de filtrage avancé des courriels entrants**, fondé sur l'analyse de l'expéditeur, du contenu et des liens présents dans le message. Les protocoles **SPF, DKIM et DMARC** doivent être configurés pour authentifier les expéditeurs et bloquer les tentatives d'usurpation du domaine de la banque.
- **Une signalétique visuelle automatique** pour les courriels provenant de l'extérieur de l'organisation : un bandeau d'alerte (« Ce message provient d'un expéditeur externe ») apparaît en tête de chaque courriel entrant, rappelant au lecteur la nécessité d'une vigilance accrue. Ce dispositif est aujourd'hui largement répandu dans les grandes entreprises.
- **Un outil intégré de signalement** dans le client de messagerie (bouton « Signaler le phishing ») permettant à chaque collaborateur de remonter en un clic un courriel suspect au service sécurité. Ce mécanisme transforme chaque salarié en capteur d'alerte et accélère considérablement le temps de détection.
- **L'authentification forte (MFA)** pour l'accès à l'ensemble des espaces sensibles, tant pour les collaborateurs (postes de travail, applications métier) que pour les clients (espace en ligne, application mobile). Même en cas de vol d'identifiants, l'attaquant ne peut accéder au compte sans le second facteur (code SMS, application d'authentification, biométrie).
- **Une surveillance active des noms de domaine proches** de celui de la banque (banquex.fr, banquex.com, banque-x.fr, etc.) afin de détecter rapidement la création

de sites frauduleux et d'engager les procédures de blocage et de retrait via les registres et les autorités compétentes.

Mesure n° 3 – Renforcer la communication et l'éducation des clients

Les clients constituent la **cible finale** des attaques de phishing : c'est leur compte que les fraudeurs cherchent à compromettre. Les protéger est à la fois une obligation morale et un enjeu de réputation pour la banque.

Plusieurs actions peuvent être mises en place :

- **Une rubrique permanente de sensibilisation** sur le site internet et l'application mobile, présentant les techniques de phishing les plus courantes, les bons réflexes à adopter et les coordonnées du service de signalement. Cette rubrique doit être visible (lien direct depuis la page d'accueil), régulièrement actualisée et illustrée d'exemples concrets.
- **Des notifications proactives** envoyées aux clients lorsqu'une campagne de phishing usurpant l'identité de la banque est détectée. Ces alertes peuvent être diffusées par SMS, par push dans l'application mobile et par bandeau d'information dans l'espace en ligne, afin d'atteindre les clients sur leurs canaux habituels.
- **Un message de prévention systématique** sur tous les supports de communication de la banque : signatures de courriels (« La banque ne vous demandera jamais vos identifiants par courriel »), reverso des relevés de compte, écrans des distributeurs automatiques, plaquettes commerciales. La répétition de ce message simple sur tous les canaux finit par installer un réflexe de méfiance face à toute sollicitation d'identifiants.
- **Une ligne téléphonique dédiée** au signalement et au conseil en cas de doute, avec un numéro court et mémorisable, accessible 24h/24. Les clients doivent pouvoir vérifier instantanément, par téléphone, la légitimité d'un courriel ou d'un SMS reçu.

Une démarche pédagogique adaptée aux publics fragiles : ateliers en agence pour les seniors, supports vidéo simples diffusés sur les réseaux sociaux, partenariats avec des associations de consommateurs. Les profils les moins familiers du numérique sont aussi les plus exposés et méritent une attention particulière.