

# Sécurité informatique –

Une étude empirique  
relative à la propension individuelle à  
divulguer des données personnelles

## Rapport de synthèse

Georges Steffgen  
et  
André Melzer

Novembre 2008



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG  
Ministère de l'Économie  
et du Commerce extérieur



# Sommaire

	<b>Page</b>
Remerciements	3
Résumé	4
<b>1 Question posée par l'étude</b>	<b>5</b>
<b>2 Description de l'étude</b>	<b>6</b>
2.1 Objectifs de l'étude	6
2.2 Méthode scientifique	6
2.2.1 Conception et réalisation de l'étude	6
2.2.2 Instrument de mesure : questionnaire	7
2.2.3 Description de l'échantillon	8
2.2.4 Analyse statistique des données	8
<b>3 Résultats de l'étude empirique</b>	<b>9</b>
3.1 Étendue et forme de l'utilisation d'un mot de passe	9
3.2 Connaissance de mots de passe d'autrui	10
3.2 Divulgence du propre mot de passe	10
3.4 Divulgence d'autres données personnelles	13
<b>4 Conclusions</b>	<b>14</b>

## Remerciements

Les auteurs de ce rapport tiennent à remercier le Ministère de l'Économie et du Commerce extérieur et ses collaborateurs chargés du Portail de la sécurité de l'information CASES (François Thill, Pascal Steichen, Gabi Rapp), ainsi que la société luxembourgeoise P&T, la Ville de Luxembourg et la Luxexpo SA pour leur précieuse collaboration. Lors de la réalisation de cette étude, les auteurs ont bénéficié du soutien énergique des étudiants en psychologie Sarah Wilkins, Astrid de Leeuw, Melissa Roll, Christian Schwager-Pérez, Manuel Spitzley et Andreas Vuori.

Un remerciement particulier est en outre adressé à toutes les personnes interrogées, sans lesquelles la réalisation de cette étude n'aurait pas été possible.

## Résumé

Le présent rapport de synthèse présente les premiers résultats d'une étude empirique. Sur requête du Ministère de l'Économie et du Commerce extérieur de Luxembourg et en collaboration avec celui-ci, l'unité de recherches INSIDE de l'Université du Luxembourg a effectué un sondage afin de déterminer la propension individuelle à divulguer des données personnelles. L'objectif principal était de déterminer la fréquence avec laquelle des personnes sont disposées à révéler leur propre mot de passe valide, ceci en tenant compte de trois conditions de sondage différentes. Les personnes interrogées n'ont soit pas reçu de récompense, soit reçu une petite récompense (une tablette de chocolat) au début ou à la fin du questionnaire. Un questionnaire concis et standardisé a été développé en se fondant sur un précédent sondage relatif au même sujet effectué au Royaume-Uni. Six enquêteurs ont effectué le sondage auprès d'un total de 1040 personnes au cours de la Foire d'automne (Foire ; n=524) et dans la Ville de Luxembourg (n=516). Outre l'étendue et la forme de l'utilisation d'un mot de passe ainsi que la connaissance de mots de passe d'autrui, il s'agissait en particulier de déterminer la propension à divulguer son propre mot de passe et d'autres données personnelles.

Une première analyse descriptive statistique des données recueillies indique que 23,4 % des personnes interrogées divulguent de bon gré leur mot de passe si on le leur demande. 9,6 % des personnes ont, de plus, fourni au cours du sondage suffisamment d'informations pour permettre une extrapolation aisée de leur mot de passe. Chez 15,8 % des sondés, le mot de passe peut être déterminé par le biais de recherches peu fastidieuses. Seulement environ la moitié des personnes interrogées (51,2 %) refuse de divulguer son mot de passe ou d'éventuelles indications quant à celui-ci. Il s'avère par ailleurs que les personnes ayant reçu une récompense pour leur participation au sondage sont plus enclines à révéler leur mot de passe ( $\text{Chi}^2=4.35$ ;  $p<.05$ ).

Les résultats indiquent dans l'ensemble que des mesures supplémentaires sont nécessaires afin d'inciter les utilisateurs des nouvelles technologies de l'information et de la communication à adopter un comportement sécuritaire adéquat.

# 1 Question posée par l'étude

Assurer la sécurité de l'information dans le cadre de l'emploi des nouvelles technologies de l'information et de la communication représente désormais un défi majeur, tant pour les fournisseurs que pour les utilisateurs de ces technologies.

La multitude de possibilités offertes, par exemple par l'internet, cache souvent une quantité non moins importante de dangers et de risques. La professionnalisation croissante de la cybercriminalité avec ses formes d'attaques sophistiquées représente une réelle menace. Un ordinateur ne disposant pas d'une protection adéquate devient ainsi facilement la proie des criminels. Ceux-ci sont alors en mesure de s'approprier diverses données personnelles qui y sont stockées. Ces risques sont d'autant plus grands que les utilisateurs de postes de travail informatiques ne sont souvent pas conscients des dangers et qu'ils omettent d'appliquer les principales règles de sécurité lorsqu'ils utilisent leur ordinateur.

À cet égard, l'utilisation des *mots de passe* constitue l'un des principaux problèmes. L'accès aux mots de passe d'autrui permet de s'introduire sans difficulté dans des systèmes informatiques et d'y provoquer des dommages. CASES (Cyberworld Awareness and Security Enhancement Structure), un service du Ministère de l'Économie et du Commerce extérieur chargé de l'amélioration de la sécurité de l'information a ainsi déterminé, dans le cadre de ses activités, qu'un grand nombre d'utilisateurs n'accorde pas l'attention nécessaire à l'utilisation de leurs mots de passe.

La question qui découle de ces observations pour CASES est la suivante : dans quelle mesure des personnes sont-elles disposées à révéler des données personnelles dans des situations précises ? C'est également la question de départ de la présente étude.

## 2 Description de l'étude

### 2.1 Objectifs de l'étude

En raison du peu de données disponibles relatives à la sécurité de l'information pour le Luxembourg, cette étude avait pour objectif principal de déterminer la propension individuelle d'une personne à divulguer son propre mot de passe à des tiers.

### 2.2 Méthode scientifique

Un groupe de travail a été créé pour la réalisation de l'étude. Celui-ci a d'une part élaboré un questionnaire adapté au contexte luxembourgeois et, d'autre part, recruté des enquêteurs, les a formés et les a encadrés pendant la durée de l'étude.

Les attributions de l'unité de recherches INSIDE comportaient de plus : l'élaboration d'un protocole d'étude, l'analyse des données recueillies ainsi que la présentation des principaux résultats (rapport de synthèse). Dans le cadre d'une analyse statistique exhaustive des données, un rapport final détaillé sera en outre établi ultérieurement.

#### 2.2.1 Conception et réalisation de l'étude

La propension observable au Luxembourg à divulguer des données personnelles (sensibles) devait être établie dans le cadre de cette étude. À cet effet, une conception quasi expérimentale a été élaborée, un plan factoriel (3x2) avec groupes aléatoires a été établi (facteur 1 : récompense – 3 conditions ; facteur 2 : lieu – 2 conditions).

En ce qui concerne le facteur 1, 3 conditions différentes ont été définies. La moitié des sondés n'a pas reçu de récompense (« neutre »), un quart des personnes interrogées a reçu une tablette de chocolat dès le début du questionnaire (« récompense immédiate ») et le dernier quart des sondés a reçu une récompense annoncée au début du questionnaire mais seulement à la fin de celui-ci (« récompense retardée »).

La totalité des personnes a été questionnée au cours de la période allant du 18 au 26 octobre 2008. Une répartition égalitaire des genres a été observée (même nombre d'hommes et de femmes). La sélection des enquêteurs a également été effectuée de manière à garantir une répartition égalitaire des genres (trois étudiantes bachelor et trois étudiants bachelor en psychologie de l'Université du Luxembourg). Les enquêteurs sélectionnés pouvaient être qualifiés de moyennement à très attirants. Chacun d'eux portait ostensiblement un badge nominatif comportant le logo de l'Université du Luxembourg au cours du sondage. Le sérieux de leur démarche était de plus souligné par leur tenue vestimentaire (vêtements « affaires », p. ex. costume et cravate).

Le sondage a été effectué oralement, à l'aide d'un questionnaire standardisé. Pour participer au sondage, les personnes questionnées devaient être salariées et travailler sur poste de travail informatique.

### 2.2.2 Instrument de mesure : questionnaire

Le questionnaire utilisé était rédigé en allemand et en français et a été élaboré en se fondant sur un instrument de mesure développé au Royaume-Uni et adapté au contexte luxembourgeois.

Le questionnaire était constitué d'un total de 17 questions. Le volume et le contenu étaient largement dictés par la durée fixée (il devait être réalisable en deux à trois minutes). Le questionnaire complet figurera en annexe du rapport final à rédiger.

Le questionnaire devait aider à déterminer : l'étendue et la forme de l'utilisation d'un mot de passe, la connaissance de mots de passe d'autrui et, en particulier, la

propension à divulguer son propre mot de passe ainsi que d'autres données personnelles.

### 2.2.3 Description de l'échantillon

L'échantillon obtenu de N=1040 sondés est décrit comme suit.

Lors du sondage, 50,4 % des personnes interrogées se trouvaient sur le site du parc des expositions à l'occasion de la Foire d'automne et 49,6 % se trouvaient au centre-ville de Luxembourg.

L'échantillon présente également une répartition égalitaire en ce qui concerne les genres (50,1 % de femmes et 49,9 % d'hommes).

43 % des sondés ont été questionnés en français, 35 % en allemand et 22 % en luxembourgeois.

### 2.2.4 Analyse statistique des données

Les questionnaires complétés ont été codés et saisis de façon anonyme par les enquêteurs. Le traitement et l'analyse des données ont été effectués à l'aide du logiciel de statistiques SPSS15 pour Windows. À l'issue de mesures de contrôle et de tests de vraisemblance, une analyse descriptive statistique des données a été réalisée en vue de la rédaction du présent rapport de synthèse. Celle-ci tient compte de la répartition proportionnelle des réponses des sondés aux différentes questions ainsi que de premiers tests de signification ( $\text{Chi}^2$ ).

La répartition proportionnelle des données permet de formuler des premières conclusions se révélant également accessibles pour le profane en matière de statistiques.

Des analyses plus exhaustives seront présentées dans le cadre de la rédaction d'un second rapport final plus détaillé.

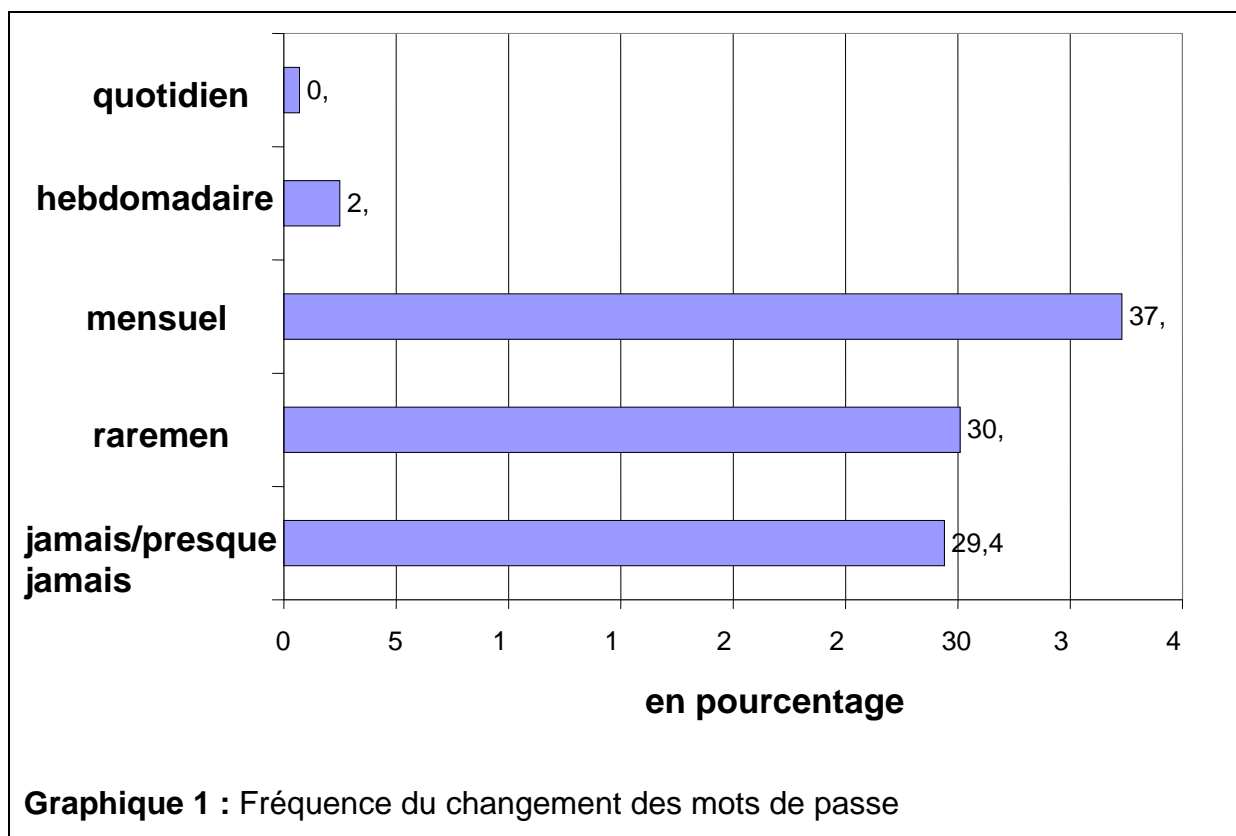
### 3 Résultats de l'étude scientifique

#### 3.1 Étendue et forme de l'utilisation d'un mot de passe

À la question relative à l'utilisation d'un mot de passe au niveau de leur poste de travail, 92,4 % des sondés répondent par l'affirmative. 7,6 % indiquent ne pas utiliser de mot de passe.

Dans le cas où un mot de passe est utilisé, 36,6 % des sondés n'en utilisent qu'un seul, 36,3 % deux ou trois, 14,4 % quatre ou cinq, 10,7 % six à dix et 11 % plus de dix.

Questionnés sur la fréquence avec laquelle ils changent leur mot de passe, un total de 59,5 % des sondés déclarent changer leur mot de passe rarement ou ne jamais en changer (voir graphique 1).



32,8 % des personnes interrogées utilisent le même mot de passe pour différentes applications. Parmi les 67,2 % qui utilisent des mots de passe différents, 33,8 % des sondés en utilisent deux ou trois, 27,9 % quatre ou cinq, 29 % six à dix et 9,3 % plus de dix.

## 3.2 Connaissance de mots de passe d'autrui

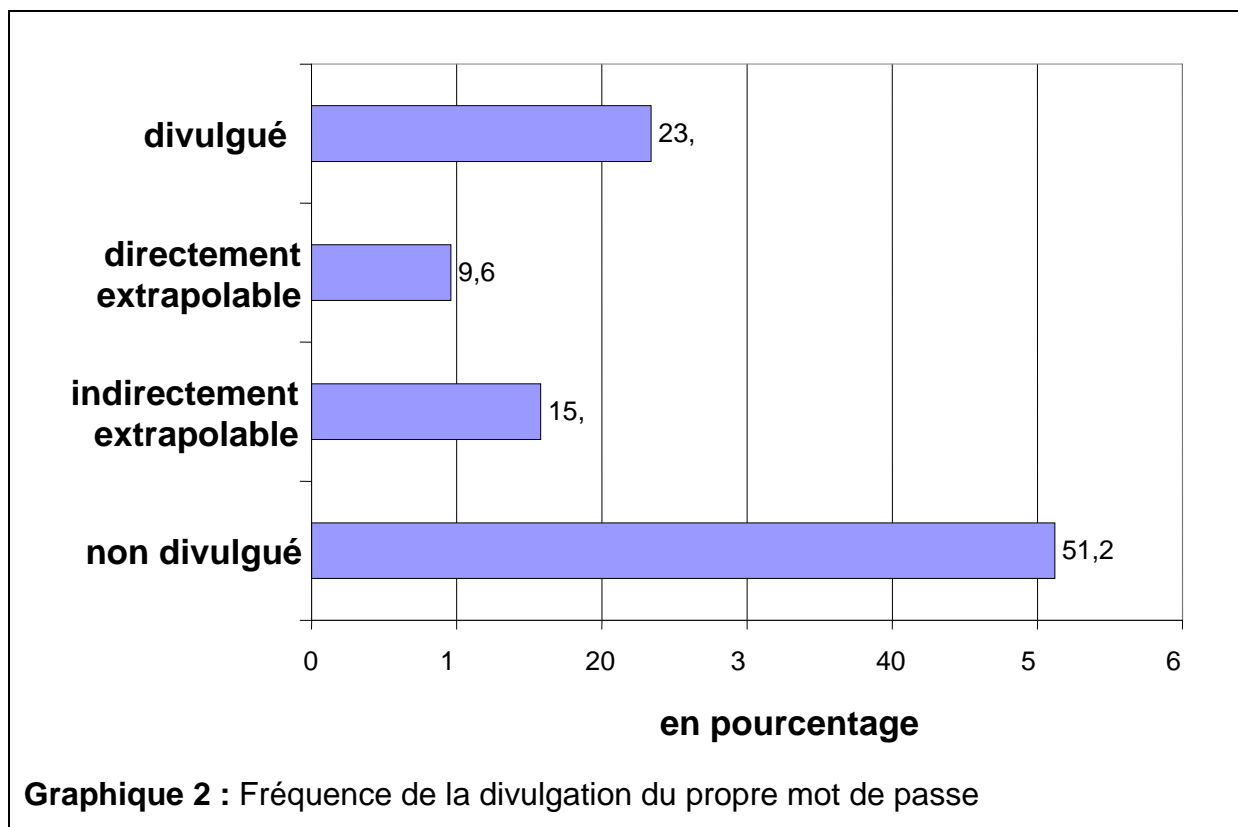
Interrogés sur leur connaissance des mots de passe de leurs collègues, 25,5 % des personnes déclarent le connaître. Parmi les sondés déclarant avoir connaissance de mots de passe d'autrui, 28,4 % disent connaître un mot de passe, 35,4 % deux ou trois, 15,6 % quatre ou cinq, 8,7 % six à dix et 2,7 % plus de dix.

## 3.3 Divulgence du propre mot de passe

22,9 % des sondés sont disposés à communiquer leur mot de passe sur demande émanant du service informatique de leur entreprise.

24,7 % des personnes questionnées ont communiqué leur mot de passe à des collègues. Parmi les personnes n'ayant pas encore communiqué leur mot de passe à des collègues, 28,9 % sont disposés à le faire si on leur demande.

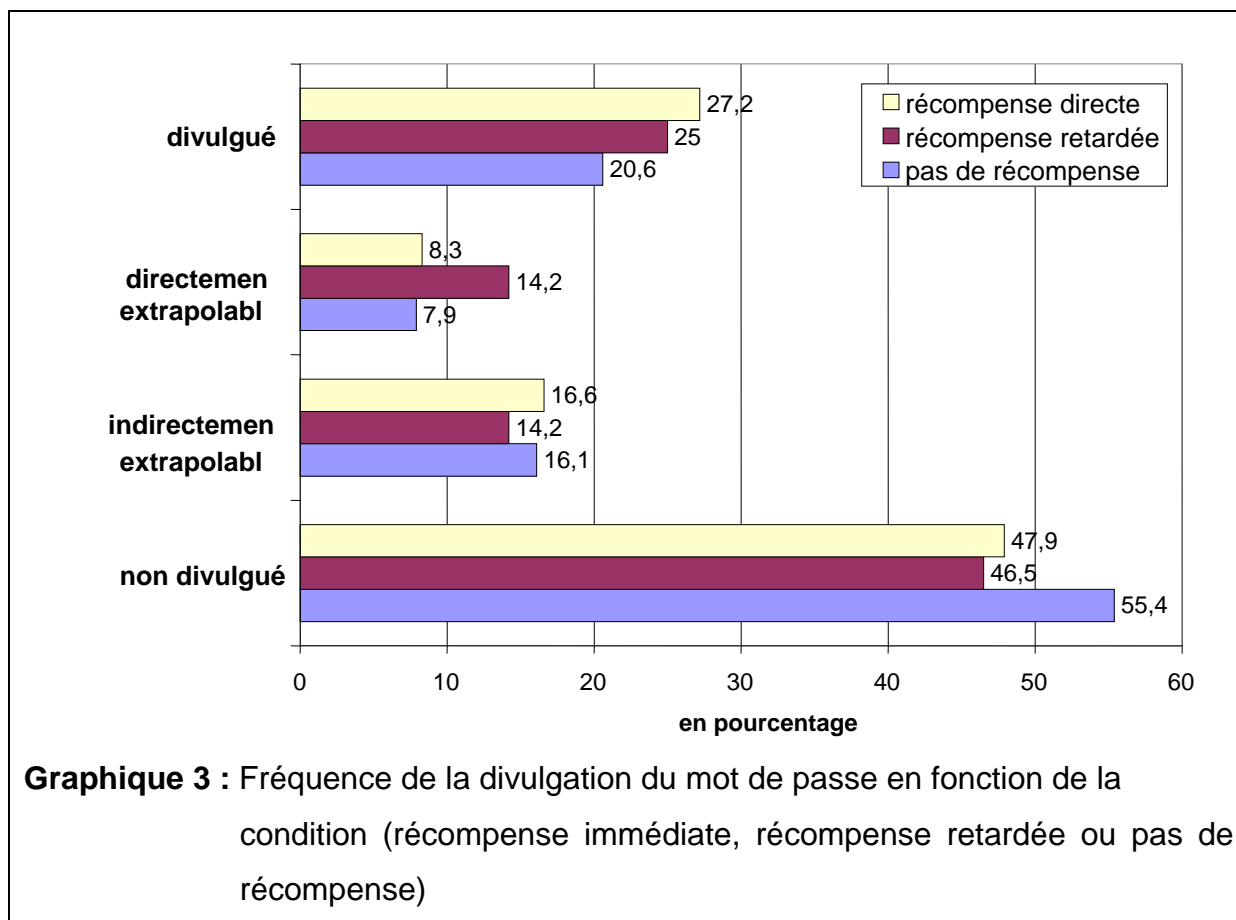
Concrètement, quelle est la proportion de sondés disposés à révéler leur mot de passe directement à l'enquêteur (voir graphique 2) ?



Le graphique 2 permet de constater qu'un total de 23,4 % des sondés sont disposés à révéler leur mot de passe sur simple demande. Parmi les personnes questionnées ne divulguant pas directement leur mot de passe, celui-ci est directement extrapolable à partir des données révélées au cours du questionnaire dans 9,6 % des cas. Chez 15,8 % des sondés, le mot de passe peut être déterminé par le biais de recherches peu fastidieuses.

Seulement environ la moitié des personnes interrogées (51,2 %) refuse de divulguer son mot de passe ou d'éventuelles indications quant à celui-ci.

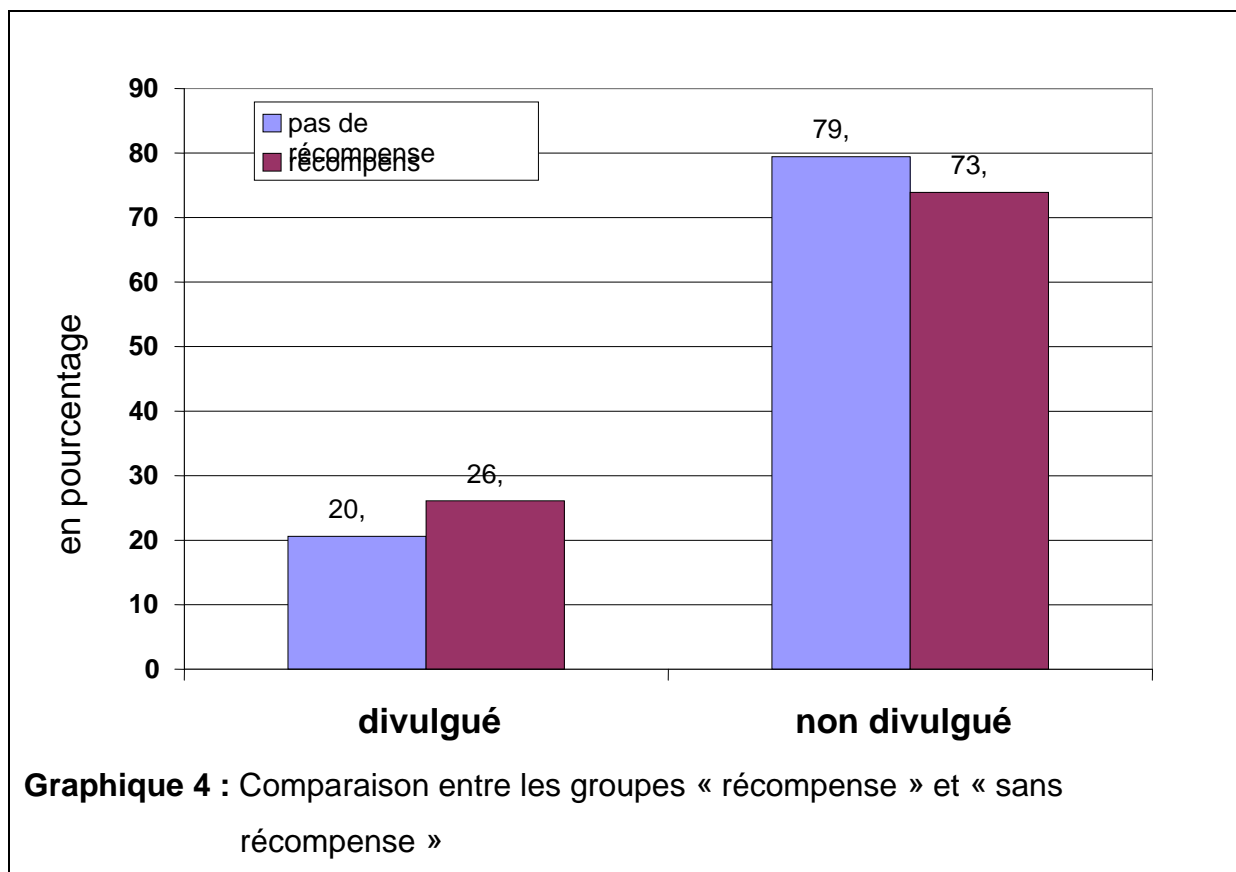
Dans quelle mesure les conditions du sondage ont-elles généré des différences au niveau des réponses des sondés ? La récompense a-t-elle une influence sur les réponses ?



La comparaison graphique des trois conditions démontre que les sondés ayant reçu une récompense directe (27,2 %) et ceux ayant reçu une récompense retardée (25 %) divulguent plus fréquemment leur mot de passe que ceux n'ayant pas reçu de récompense (20,6 %). Les différences perceptibles dans le graphique 3 sont-elles significatives d'un point de vue statistique ?

Différentes analyses statistiques démontrent que les deux groupes ayant reçu une récompense ne divergent pas substantiellement (voir graphique 3). Pour cette raison, les deux groupes ayant reçu une récompense (immédiate ou retardée) ont été réunis pour former le groupe « récompense ».

Une comparaison statistique entre les sondés ayant reçu une récompense et ceux n'ayant pas reçu de récompense révèle alors une différence significative ( $\text{Chi}^2=4.35$ ;  $p<.05$ ). Les personnes ayant reçu une récompense (26,1 %) sont nettement plus enclines à révéler leur mot de passe que celles n'ayant pas reçu de récompense (20,6 % – voir graphique 4).



Dans ce contexte, le genre des personnes questionnées ainsi que le lieu de sondage ne semblent pas jouer de rôle important. Dans le groupe « récompense », 24,8 % des hommes et 27,4 % des femmes questionnés révèlent leur mot de passe, alors que sans récompense, 19,1 % des hommes et 22,0 % des femmes sont disposés à le divulguer. Les sondés ayant reçu une récompense ont révélé leur mot de passe à 26,8 % sur le site de la Foire d'automne et à 25,4 % au centre-ville. En absence de récompense, 21,0 % des personnes questionnées sur le site de la Foire d'automne révèlent leur mot de passe pour 20,1 % au centre-ville.

### 3.4 Divulgation d'autres données personnelles

En moyenne, 23,4 % des sondés sont donc disposés à divulguer leur mot de passe à une personne inconnue. De plus, 63,4 % des personnes questionnées sont

disposées à donner des indications quant à leur mot de passe. Seulement 13,2 % des sondés ne fournissent ni mot de passe, ni indication à son sujet.

Quelles sont les indications données par les sondés ? 12,6 % ont déclaré qu'il s'agissait du nom d'un membre de la famille, 7 % qu'il s'agissait du propre nom, 5,9 % du nom d'un animal de compagnie, 5,5 % d'une date de naissance, 1,5 % du nom d'une vedette, 0,9 % d'une marque de voiture et 66,6 % ont donné d'autres indications.

À la fin du sondage, 89,1 % des personnes interrogées communiquaient leur date de naissance, 79,5 % donnaient leur nom et 57,8 % leur numéro de téléphone.

## 4 Conclusions

Quelles conclusions peut-on formuler sur la base des présents résultats ? Les données indiquent que près d'un quart des sondés (23,4 %) est disposé à révéler directement son mot de passe et que ce comportement peut être favorisé par la remise d'une petite récompense – une tablette de chocolat. La récompense joue alors un rôle plus important que le genre ou le lieu du sondage.

La présente étude permet de démontrer à quel point il est aisé d'obtenir un accès important à des données personnelles. Ces résultats démontrent qu'il est nécessaire de prendre d'urgence des mesures ciblées sur les personnes afin de renforcer le comportement sécuritaire des utilisateurs en matière de sécurité de l'information.