*Baromètre Euler Hermes-DFCG 2020*

# Plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude cette année

- Le risque de fraude et de cybercriminalité ne faiblit pas : en 2019, plus de 7 entreprises sur 10 ont subi au moins une tentative de fraude (comme en 2018)
- Les fraudeurs multiplient les attaques sur une même cible pour augmenter leurs chances de réussite : près d'une entreprise sur 3 a subi plus de 5 tentatives de fraude en 2019 (1/4 en 2018)
- L'usurpation d'identité reste la technique privilégiée par les fraudeurs, suivie par la cyber-fraude et la fraude interne

**PARIS, 12 MAI 2020** – Face à la situation économique et sanitaire inédite que nous vivons, les entreprises ont une priorité clairement définie : préserver la continuité de leur entreprise. Si leur attention est pleinement focalisée sur cet enjeu essentiel, d'autres risques peuvent affecter fortement leur structure à court terme. Parmi ces risques, une menace tend à se renforcer ces dernières semaines : le risque de fraude et de cybercriminalité. En effet, la période actuelle ouvre aux fraudeurs de nouvelles brèches pour parvenir à leurs fins.

Dans ce contexte, pour la 6ème année consécutive, Euler Hermes, le leader européen de l'assurance fraude, et l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG), ont interrogé plus de 200 entreprises implantées en France sur leur exposition, leur ressenti et leurs mesures de prévention face aux risques de fraude et cybercriminalité. Décryptage des résultats de ce baromètre annuel.

## Le risque de fraude et de cybercriminalité reste toujours aussi intense

En 2019, plus de 7 entreprises sur 10 ont été victimes d'au moins une tentative de fraude. Un chiffre similaire à celui constaté en 2018 et en 2017, preuve de la résilience des fraudeurs: ces derniers maintiennent une pression intense sur les entreprises françaises. Plus inquiétant encore, la récurrence de ces attaques sur une même cible. En effet, en 2019, 29% des répondants à l'enquête Euler Hermes-DFCG ont été visés par plus de 5 tentatives (24% en 2018). Les fraudeurs n'hésitent pas à revenir à la charge constamment, jusqu'à ce que le système de défense de leur cible cède.

Malheureusement, cette persévérance porte ses fruits : 27% des entreprises interrogées ont subi au moins une fraude avérée en 2019, soit une légère progression (26% en 2018). Comment expliquer cette efficacité croissante ? Le moment de l'attaque est un premier élément : 43% des entreprises ont remarqué une recrudescence des attaques en période de congés, week-end ou veille de week-end (35% en 2018). Les fraudeurs concentrent leurs efforts sur les périodes où les entreprises sont les moins armées pour se protéger (moins de personnel, moins d'attention, etc).

Mais subir une fraude, combien cela coûte-t-il concrètement ? La facture se révèle généralement assez salée : pour près d'une entreprise sur 3, le préjudice subi est supérieur à 10K€ (comme en 2018). De quoi fragiliser fortement la trésorerie des entreprises et dans certains cas compromettre leur activité, plus encore dans le contexte actuel où les chaînes d'approvisionnement sont perturbées et la demande à l'arrêt.

## L'usurpation d'identité reste la technique préférée des pirates devant les outils cyber

L'usurpation d'identité est la technique plébiscitée par les fraudeurs, citée 4 fois parmi le top 5 du baromètre Euler Hermes – DFCG. La fraude au faux fournisseur est toujours la plus utilisée par les pirates, citée par 48% des répondants. Elle est suivie par la fraude au faux président, qui a sensiblement progressé (38%), les autres usurpations d'identité (banques, avocats, commissaires au compte – 31%) et la fraude au faux client (24%).

*« L'usurpation d'identité est un grand classique de la fraude, et elle est de loin la technique favorite des fraudeurs. Son usage a toutefois évolué : là ou auparavant, le mail était le facteur déclencheur, de nouvelles techniques plus pointues sont apparues et permettent aux fraudeurs de gagner en efficacité. On peut notamment penser à l'intelligence artificielle et aux logiciels d'imitation de voix, grâce auxquels les fraudeurs ont plus de crédibilité dans leurs tentatives, et qui permettent de constituer des scénarios d'usurpation d'identité extrêmement convaincants »*, explique Armelle Raillard, Experte assurance-fraude chez Euler Hermes France.

Par ailleurs, l'intrusion dans les systèmes d'information (29%) apparait également dans le top 5. Elle est utilisée à la fois en tant qu'attaque directe, avec les rançongiciels (cités par 15% répondants), mais aussi comme un moyen de préparer une fraude. Enfin, la fraude interne a été plus utilisée en 2019 qu'en 2018, citée par 14% des répondants (12% en 2018).

**Les entreprises ont de plus en plus peur de subir une fraude ou une cyberfraude**

Les entreprises semblent de plus en plus conscientes de la menace qui plane. En effet, 84% des répondants craignent une accentuation du phénomène sur l'année à venir (+6 points par rapport à notre dernière enquête).

Christian Laveau, Président du Groupe de travail Cyberfraude de la DFCG, indique : *« Les entreprises et leurs directions financières doivent veiller à la robustesse de leurs dispositifs de contrôle interne et de lutte contre la cyberfraude. Le risque est que la crise que nous traversons conduise à une moindre vigilance ou à la « dégradation temporaire » des dispositifs de contrôle en raison de la priorité, légitime, donnée à la continuité d'exploitation. Les cyber-fraudeurs peuvent en profiter pour exploiter toute faille du dispositif de prévention et de contrôle et accentuer leurs attaques. »*

**Des mesures concrètes de défense ont été prises, mais sont-elles suffisantes ?**

La prise de conscience des entreprises est rassurante, d'autant qu'elle semble aller plus loin que la simple crainte. En effet, 60% des entreprises interrogées ont mis en place une cartographie des risques. Mieux encore : 93% d'entre elles ont identifié sur cette cartographie le risque de fraude, et 78% ont répertorié le risque de cybercriminalité. La preuve que ces menaces sont bien considérées comme un fléau par les entreprises. Certaines entreprises ont, de ce fait, décidé de créer ou transférer un budget dédié à la lutte contre la fraude. Elles sont près de 40% selon l'enquête Euler Hermes – DFCG.

Philippe Guillaumie, Président du Comité Scientifique de la DFCG précise : *« La mise en place du télétravail à grande échelle dans le cadre de la crise sanitaire a ouvert de nouvelles brèches du fait du développement des solutions numériques et illustre de nouveau la grande vulnérabilité des entreprises à la cyberfraude. Dans ce contexte, les dispositifs de contrôle interne doivent être maintenus ou renforcés, y compris dans ces circonstances exceptionnelles vis à vis du risque accentué de fraude interne, mais un investissement significatif doit être aussi consenti pour tester régulièrement la résistance des Systèmes d'Information face à la cyberfraude et identifier/réparer les failles possibles. Le recours à l'assurance est également un dispositif de protection efficace, mais il ne dispense pas d'une politique de prévention. »*

Autre motif d'optimisme, 60% des entreprises disposent désormais d'un plan d'urgence à activer en cas d'attaque, alors qu'elles n'étaient que 50% lors de la précédente édition de notre baromètre. Une amélioration notable, qui prouve que la lutte contre la fraude est un sujet pris en compte par les entreprises. Mais l'est-il assez ?

*« Il y a du mieux, et les entreprises s'en félicitent : elles sont 74% à juger leur dispositif défense satisfaisant, contre 69% l'an passé. Mais il y a encore du chemin à parcourir pour que les systèmes de défenses soient optimisés : plus de 6 répondants sur 10 n'ont toujours pas alloué de budget spécifique à la lutte contre fraude et la cybercriminalité pour cette année. Nous sommes sur la bonne voie, mais les entreprises doivent aller plus loin dans leur démarche pour se mettre à l'abri des attaques. Des dispositifs comme l'assurance-fraude existent, et permettent aux entreprises de transférer ce risque majeur sur une tierce partie pour ne pas avoir à l'assumer entièrement »*, conclut Armelle Raillard.

**********

**Contacts médias**

**EULER HERMES FRANCE**
Maxime Demory +33 (0)1 84 11 35 43
maxime.demory@eulerhermes.com

**DFCG**
Charles Bonati +33 (0)1 40 20 94 50
charlesbonati@dfcg.asso.fr

**VAE SOLIS COMMUNICATIONS**
Anaïs Agozo Ndelia +33 (0)1 80 48 14 80
aagozondelia@footprintconsultants.fr

**Réseaux sociaux**

- Suivez-nous sur Twitter : @eulerhermesFR et @dfcgasso
- Suivez-nous sur LinkedIn : Euler Hermes France et DFCG
- Suivez-nous sur YouTube : Euler Hermes France

## A propos d'Euler Hermes

Prévoir les risques commerciaux et d'impayés aujourd'hui, c'est protéger la trésorerie demain. Euler Hermes est le leader mondial des solutions d'assurance-crédit et un spécialiste reconnu dans les domaines du recouvrement et de la caution. Avec plus de 100 ans d'expérience, Euler Hermes offre une gamme complète de services pour la gestion du poste clients. Son réseau international de surveillance permet d'analyser la stabilité financière de PME et de grands groupes actifs dans des marchés représentant 92% du PNB global. Basée à Paris, la société est présente dans plus de 50 pays avec plus de 5 800 employés. Membre du groupe Allianz, Euler Hermes est noté AA par Standard & Poor's. La société a enregistré un chiffre d'affaires consolidé de 2,9 milliards d'euros en 2019 et garantissait 950 milliards d'euros de transactions commerciales dans le monde fin 2019. Plus d'informations: eulerhermes.com


## A propos de la DFCG

L'Association nationale des Directeurs Financiers et de Contrôle de Gestion, créée en 1964, constitue la communauté de référence des professionnels des directions financières d'entreprises privées ou des services publics. La DFCG rassemble, dans 14 régions, 3 000 dirigeants financiers d'entreprises de toute taille, représentatives du tissu économique français. La DFCG regroupe 1 800 sociétés (Grands groupes 13%, ETI-PME 70%, TPE 17%). Depuis 2020, l'association est présidée par Daniel Bacqueroët, vice-président finance de Brink's Global Services.

- Lieu de recherche opérationnelle en finance et contrôle de gestion, ses recherches donnent matière à une dizaine de publications annuelles. Ses prises de positions contribuent au débat économique et financier.
- Sphère pédagogique pour développer les compétences de ses membres, le Centre de Formation de la DFCG propose 90 formations allant de la sensibilisation pour dirigeant aux responsabilités nouvelles, à l'expertise plus pointue en financement ou en contrôle de gestion.
- Lieu de partage de bonnes pratiques et espace d'échanges et de business, la DFCG organise plus de 500 manifestations régionales et nationales. Financium, son grand congrès annuel rassemble en décembre plus de 1 000 professionnels.
- Espace de développement professionnel, l'association s'est notamment dotée de groupes transversaux pour accompagner ses adhérents à chaque instant de leur vie professionnelle.
- 22 groupes de travail, dont le groupe Cyberfraude présidé par Christian Laveau

unknown risks and uncertainties. Actual results, performance or events may differ materially from those expressed or implied in such forward-looking statements. Such deviations may arise due to, without limitation, (i) changes of the general economic conditions and competitive situation, particularly in the Allianz Group's core business and core markets, (ii) performance of financial markets (particularly market volatility, liquidity and credit events), (iii) frequency and severity of insured loss events, including from natural catastrophes, and the development of loss expenses, (iv) mortality and morbidity levels and trends, (v) persistency levels, (vi) particularly in the banking business, the extent of credit defaults, (vii) interest rate levels, (viii) currency exchange rates including the euro/US-dollar exchange rate, (ix) changes in laws and regulations, including tax regulations, (x) the impact of acquisitions, including related integration issues, and reorganization measures, and (xi) general competitive factors, in each case on a local, regional, national and/or global basis. Many of these factors may be more likely to occur, or more pronounced, as a result of terrorist activities and their consequences.