



Die  
Bundesregierung

---

6 mars 2024

---

# Foire aux questions

Protection des élections européennes contre les menaces hybrides, y compris la désinformation

## Sommaire

---

1.Pourquoi faut-il protéger les élections européennes ?	3
2.Que sont les menaces hybrides ?	3
3.Qu'est-ce que la désinformation ?	4
4.Quel est le niveau de menace évalué par le gouvernement fédéral à l'approche des élections européennes de 2024 ?	4
5.Quels moyens d'influence illégitime peuvent être utilisés par des États étrangers ?	5
6.Que fait le gouvernement fédéral pour protéger les élections européennes contre l'influence illégitime d'États étrangers ?	6
7.Comment le gouvernement fédéral réagit-il aux éventuelles informations fausses ou trompeuses concernant le déroulement des élections européennes ?	7
8.Est-ce que le déroulement des élections européennes est sûr et est-ce que tout risque de manipulation lors du vote et du dépouillement peut être exclu ?	7
9.De quelle manière l'UE garantit-elle la liberté et l'équité des élections européennes ?	8
10.Comment identifier les informations fausses et trompeuses et se protéger contre la désinformation ?	9
11.Où trouver plus d'informations ?	10

---

# Protection des élections européennes contre les menaces hybrides, y compris la désinformation

## 1. Pourquoi faut-il protéger les élections européennes ?

**Du 6 au 9 juin 2024, les citoyennes et citoyens de l'Union européenne (UE) vont élire pour la dixième fois le Parlement européen.** Ce vote leur permet de désigner les députés qui les représentent au Parlement européen. Ils décident ainsi pour une large part de l'orientation de la politique de l'UE dans les années à venir. **Pour l'Allemagne, l'élection aura lieu le dimanche 9 juin 2024.** L'élection du Parlement européen est soumise à la réglementation électorale de chaque pays. En Allemagne, cette élection est un scrutin national.

La sécurité du déroulement et la garantie des élections parlementaires est d'une importance capitale pour notre démocratie. La neutralité des organes électoraux, imposée par la loi, ainsi que le principe d'élection publique, garanti par la Constitution, sont des conditions fondamentales pour que la population ait confiance dans l'organisation des élections et en accepte le résultat. Toutes les étapes essentielles de l'élection sont contrôlables par le public.

**Les élections sont l'élément central de la démocratie et, en tant que telles, méritent une protection particulière. Les élections doivent notamment être protégées contre l'influence illégitime d'États étrangers.** Les élections sont fréquemment l'objet d'activités illégitimes renforcées de la part d'États étrangers. En effet, attiser la peur et propager la haine peuvent contribuer à la polarisation de la société et influencer le comportement électoral. Certains États, en particulier des autocraties, tentent délibérément de mettre en doute la légitimité de nos élections et d'affaiblir la confiance de nos citoyennes et citoyens dans les processus et institutions démocratiques. Ces menaces doivent être résolument combattues.

## 2. Que sont les menaces hybrides ?

**On entend par menaces hybrides différentes formes d'influence illégitime exercée sur des États par des États étrangers.** Ces États étrangers tentent, notamment par l'intermédiaire d'acteurs non étatiques, d'imposer leurs objectifs contre nos intérêts et nos valeurs, ouvertement ou non, grâce à l'utilisation coordonnée de différents instruments. Ces agissements visent à déstabiliser et affaiblir notre démocratie. **Parmi les instruments employés, on compte notamment la désinformation, les cyberattaques contre des services étatiques et des entreprises, l'espionnage, l'ingérence économique, par exemple à travers des investissements ciblés dans les industries clés et le sabotage d'infrastructures critiques.**

Les menaces hybrides concernent tous les niveaux politiques et sociétaux. Différents moyens (diplomatiques, militaires, économiques ou technologiques) peuvent être combinés de manière à former une campagne coordonnée. Il est parfois difficile d'identifier certains événements isolés comme appartenant à une large campagne et donc de réagir à temps.

### 3. Qu'est-ce que la désinformation ?

**La désinformation est une information fausse ou trompeuse diffusée de manière ciblée.** Il faut distinguer ces informations des informations fausses ou trompeuses générées et diffusées par erreur et sans intention de tromper.

Les personnes qui diffusent de la désinformation ont pour but de duper les destinataires et de les inciter à propager des informations fausses et trompeuses. La désinformation est l'œuvre d'acteurs non étatiques nationaux et étrangers ainsi que d'acteurs étatiques étrangers agissant pour différents motifs.

**Si la désinformation est diffusée par un État étranger dans le but d'exercer une influence illégitime sur un autre État (ou sur une union d'États), il s'agit dans ce cas d'une menace hybride.** Elle vise à influencer la formation de l'opinion publique, à dissimuler ses propres activités et à en détourner l'attention, à rendre émotionnels des débats controversés, à renforcer les tensions au sein de la société et/ou à exacerber la méfiance à l'égard des institutions publiques et de l'action gouvernementale, l'objectif étant de renforcer sa propre position et d'imposer ses propres intérêts.

**Les réseaux numériques mondiaux facilitent la diffusion rapide et très ciblée de la désinformation par des États étrangers.** Pour des raisons politiques, des informations sont par exemple altérées ou sorties de leur contexte dans le but d'influencer les discussions publiques. C'est notamment le mode de fonctionnement des réseaux sociaux, basé sur le partage et la diffusion simple d'informations, qui permet aux informations fausses ou trompeuses de se propager rapidement et d'atteindre un très grand nombre de personnes.

**Dans l'espace informationnel, les campagnes de manipulation et d'influence étrangères sont particulièrement problématiques.** Dans ces campagnes orchestrées par l'État sur Internet, plusieurs acteurs placent et diffusent de manière coordonnée et par différents canaux les mêmes fausses informations. En outre, ces campagnes utilisent des moyens techniques qui permettent de générer artificiellement une portée et de simuler leur crédibilité. Par exemple, des sites Internet de journaux sont copiés illégalement, de faux comptes sont créés sur les réseaux sociaux et des « bots informatiques » sont utilisés pour la diffusion automatisée des contenus et la manipulation d'algorithmes de recommandation.

En outre, l'intelligence artificielle permet aujourd'hui de créer de faux enregistrements audio, image et vidéo (appelés « deepfakes ») et de faire dire ainsi à des hommes et des femmes politiques des choses qu'ils n'ont jamais dites. Pour les États étrangers, c'est un moyen supplémentaire pour influencer notre débat politique à l'aide d'informations manipulées.

### 4. Quel est le niveau de menace évalué par le gouvernement fédéral à l'approche des élections européennes de 2024 ?

Le gouvernement fédéral examine les différentes formes d'influence illégitime exercée par des États étrangers et dirigée en particulier contre les intérêts de sécurité ou la formation de la volonté souveraine de l'Allemagne. **Le gouvernement fédéral considère que, dans le contexte des élections européennes de cette année, certains États pourraient envisager de telles mesures d'influence comme possibilités d'action.** Ces États jugeront si et sous quelle forme elles seront mises en œuvre, en fonction de l'opportunité et de l'évaluation des coûts et des bénéfices.

**Dans le contexte des élections européennes, il faut s'attendre, entre autres, à une augmentation de la désinformation étrangère en Allemagne.** On peut supposer que d'autres États tenteront d'exercer une influence illégitime sur les débats publics et la formation de la volonté politique en Allemagne. Depuis le début de la guerre d'agression russe contre l'Ukraine, contraire au droit international, le gouvernement fédéral constate sur les réseaux sociaux un accroissement de la désinformation émanant d'organes russes officiels, de médias publics russes ou proches du gouvernement ainsi que de comptes proches du Kremlin.

**Aucune cyberattaque concrète visant spécifiquement les élections européennes n'est connue à l'heure actuelle. Toutefois, ces dernières années, on a pu observer dans le monde entier une large palette de cyberattaques à l'approche d'élections.** On compte parmi elles des campagnes dites de « hack-and-leak » menées contre des partis politiques et au cours desquelles des e-mails et des documents ont été volés, puis publiés, parfois après avoir été manipulés. À cela se sont ajoutées des tentatives d'attaques contre des sites Internet et des serveurs contenant des données d'électeurs ou fournissant des informations sur les élections. Depuis le début de la guerre d'agression russe contre l'Ukraine, l'hacktivisme politique s'est intensifié également en Allemagne et peut aller de pair avec des attaques visant à saturer des sites Internet ou des événements organisés par des partis.

Les multiples exemples actuels donnent à penser que la Russie, plus que tout autre pays, pourrait tenter d'exercer une influence illégitime sur la formation de l'opinion politique à l'approche des élections européennes en Allemagne, principalement au moyen de campagnes de manipulation dans l'espace informationnel. Le gouvernement fédéral garde cependant un œil attentif sur d'autres États.

## 5. Quels moyens d'influence illégitime peuvent être utilisés par des États étrangers ?

**À l'approche des élections européennes, il faut particulièrement s'attendre à des campagnes étrangères de manipulation et d'influence dans l'espace informationnel.** Des États étrangers pourraient notamment utiliser la propagation de fausses informations dans le but d'attiser les discussions émotionnelles et de dresser certains groupes de la société les uns contre les autres. Les sujets susceptibles d'être instrumentalisés sont par exemple la migration ou le changement climatique, autant de thèmes soulevant également des questions socio-économiques. **Il est possible que des informations fausses et trompeuses soient diffusées par la falsification volontaire de comptes de réseaux sociaux et de sites Internet de personnes, partis, entreprises de médias ou autorités. De plus, des images et des fichiers audio et vidéo manipulés par intelligence artificielle (appelés « deepfakes ») sont susceptibles d'être utilisés** pour influencer l'opinion publique.

**Des États étrangers peuvent également avoir recours à des cyberattaques pour préparer et soutenir les activités de désinformation. Il faut ainsi s'attendre à des opérations dites de « hack-and-leak » :** il s'agit de la publication de données et d'informations volées dans l'environnement politique. Ces publications peuvent également contenir des données falsifiées ou manipulées, visant à discréditer notamment des personnes ou des partis. **On doit également prévoir des tentatives d'accès aux comptes de réseaux sociaux et aux sites Internet de personnes, partis, entreprises de médias ou autorités dans le but de les pirater et de les utiliser pour propager de la désinformation.**

En vue de l'élection européenne organisée en Allemagne, on peut envisager une désinformation au détriment de partis ainsi que d'hommes et de femmes politiques. **L'objectif des attaques n'est**

**pas seulement d'influencer les élections au profit d'un certain parti. L'intention poursuivie consiste souvent à ébranler la confiance dans la légitimité du processus de vote et des résultats de l'élection et donc dans la démocratie en elle-même.** Dans le contexte des élections européennes, il est possible que des États étrangers pratiquent, ordonnent ou renforcent la propagation d'informations fausses ou trompeuses destinées à mettre en doute l'intégrité du scrutin et l'exactitude de ses résultats.

## 6. Que fait le gouvernement fédéral pour protéger les élections européennes contre l'influence illégitime d'États étrangers ?

**La démarche du gouvernement fédéral à l'encontre de l'influence illégitime d'États étrangers englobe l'ensemble de la société.** Tous les ministères du gouvernement fédéral ainsi que leurs secteurs d'activités sont impliqués dans cette démarche. La collaboration entre l'État fédéral et les Länder, y compris leurs communes et les autorités de sécurité, ainsi que l'échange avec la société civile, jouent un rôle essentiel. La coopération avec des États partenaires et au sein de réseaux internationaux est un autre élément important.

Sous l'égide du ministère fédéral de l'Intérieur et du Territoire (BMI), le groupe de travail sur les menaces hybrides (« AG Hybrid ») coordonne la stratégie du gouvernement fédéral en matière de menaces hybrides. Au centre de ce groupe de travail se trouve la task force interministérielle et interautorités contre la désinformation. Les activités de cette task force se concentrent avant tout sur les mesures visant à identifier les récits, à renforcer une communication proactive basée sur les faits et à améliorer la résilience de la société contre les menaces émanant de l'espace informationnel.

**Le BMI coordonne la protection de l'élection européenne en Allemagne contre les menaces hybrides, y compris la désinformation. Dans le cadre de la task force contre la désinformation dirigée par le BMI, un échange étroit a lieu entre les différents ministères et autorités.** Dans ce cadre, le BMI se concerta très intensivement avec les autorités de sécurité, la Chancellerie fédérale, le ministère fédéral des Affaires étrangères (AA) et l'Office de presse et d'information du gouvernement fédéral (BPA) au sujet du niveau de menace et des mesures à prendre pour protéger l'élection européenne en Allemagne. Les autorités échangent leurs informations respectives et réagissent en conséquence. **Cela permet d'identifier et de repousser systématiquement les activités d'influence potentielles menées par des États étrangers contre les élections européennes.** Une étroite concertation a lieu également avec le bureau de la responsable fédérale des élections et le Centre fédéral pour l'éducation civique (BpB).

**L'Office fédéral de la sécurité des technologies de l'information (BSI) soutient entre autres les responsables des élections au niveau national et dans les Länder, les candidats ainsi que les partis en matière de sécurité de l'information en leur offrant différents services d'information, d'aide et de conseil.** Cela concerne en particulier la protection des comptes de réseaux sociaux, des identités numériques et des sites Internet, l'utilisation de l'intelligence artificielle, une observation étendue de la situation et, si nécessaire, la mise en garde, la détection de logiciels malveillants et l'assistance en cas d'incident.

**Le gouvernement fédéral accorde une grande importance à la prévention et au développement d'une résilience nationale et sociétale.** La sensibilisation du public en matière de menaces hybrides et un débat sociétal portant sur le traitement de la désinformation jouent un rôle central. La promotion et le développement des compétences de toutes les tranches d'âge dans le domaine des informations et des médias ont lieu de manière ciblée. La lutte contre la désinformation dépend de chacun et chacune.

**La protection des élections européennes est également l'une des priorités de l'UE.** Les réunions du groupe de travail du Conseil consacré au renforcement de la résilience et à la lutte contre les menaces hybrides sont régulièrement le cadre d'échanges de rapports d'expérience des États membres de l'UE, d'exemples de bonnes pratiques et de résultats de recherche, notamment sur le traitement de la désinformation dans le contexte des élections.

**L'échange avec les plateformes en ligne est lui aussi un élément clé du traitement de la désinformation,** tant au niveau européen que national, les opérateurs de réseaux sociaux jouant un rôle important dans le cadre des mesures prises contre la diffusion d'informations fausses ou trompeuses.

## 7. Comment le gouvernement fédéral réagit-il aux éventuelles informations fausses ou trompeuses concernant le déroulement des élections européennes ?

**L'information, la sensibilisation et le principe d'élection publique sont les principales mesures contre la désinformation. Pour lutter contre celle-ci, la responsable fédérale des élections informe le public activement, largement et par différents moyens de communication** (notamment sur son site Internet, sur les réseaux sociaux, dans des communiqués de presse et des interviews) au sujet de la préparation et du déroulement du scrutin ainsi que sur les règles garantissant l'intégrité de l'élection et du dépouillement des votes.

La responsable fédérale des élections est la source officielle et impartiale d'informations sur la procédure électorale. Elle est chargée d'identifier et de combattre la désinformation lorsque l'information concerne son domaine de compétence ou la procédure électorale en général. Son équipe observe la situation dans les médias afin d'identifier la désinformation et de s'y opposer. **Cela comprend la rectification active des déclarations fausses ou trompeuses, diffusées par exemple sur les réseaux sociaux, sur le déroulement de l'élection européenne en Allemagne.**

**Par ailleurs, la responsable fédérale des élections coopère avec le BpB, lequel propose un large éventail d'informations sur tous les thèmes politiques et fournit différents types d'informations sur les élections européennes.** Sur ses canaux de réseaux sociaux, le BpB se penchera sur les élections européennes et traitera le sujet sous différentes formes. Le site Internet du BpB offrira un dossier consacré à la désinformation dans le contexte des élections européennes. De plus, un chatbot dédié aux élections européennes fournira des informations fiables.

## 8. Est-ce que le déroulement des élections européennes est sûr et est-ce que tout risque de manipulation lors du vote et du dépouillement peut être exclu ?

**La responsable fédérale des élections et tous les autres organes électoraux mettent en œuvre, avec le soutien du BSI, de nombreuses mesures garantissant la sécurité des élections. En outre, différents mécanismes de sécurité en matière de droit électoral assurent le déroulement en bonne et due forme du scrutin et le protègent contre les manipulations.**

Le vote, tant dans les bureaux de vote que par correspondance, se fait exclusivement avec des bulletins de vote officiels. **Les machines à voter ou les procédures de vote en ligne** utilisées dans

d'autres pays, comme les États-Unis, et qui pourraient être la cible de cyberattaques, **ne sont pas utilisées en Allemagne.**

Tant le vote au bureau de vote que l'envoi de documents de vote par correspondance sont enregistrés sur les listes électorales, de sorte que chaque électrice et chaque électeur ne peut voter qu'une seule fois. La fraude électorale est passible de sanctions pénales. Les voix exprimées dans les bureaux de vote et par correspondance sont comptées publiquement et de manière contrôlable pour tous par des volontaires bénévoles inscrits sur les listes électorales.

**Lors du calcul des résultats, seuls les communiqués rapides du résultat final provisoire publié le soir du scrutin sont transmis également sous forme électronique. La protection de ces données sensibles est assurée par une sécurité de l'information appropriée et conforme à l'état actuel de la technique.** Pour garantir le calcul correct et en temps voulu du résultat provisoire des scrutins organisés à l'échelle fédérale ainsi que pour parer aux dangers du cyberspace, un groupe de travail du BSI réunissant l'État fédéral et les Länder a élaboré dès décembre 2022, en collaboration avec l'équipe centrale des Länder et avec les responsables des élections dans les Länder et au niveau fédéral, un profil de protection de base des technologies informatiques destiné à garantir la sécurité de l'information pour le calcul des résultats provisoires de scrutins parlementaires à l'échelle fédérale (sécurité de l'information lors des communiqués rapides).

Le résultat définitif du scrutin est établi à partir des procès-verbaux des bureaux de vote, des bureaux de vote par correspondance et des commissions électorales des arrondissements et des Länder. **Toute influence des cyberattaques sur le résultat définitif officiel de l'élection est techniquement exclue.** En cas de doutes justifiés, il est possible de recompter les résultats dans les circonscriptions électorales.

## 9. De quelle manière l'UE garantit-elle la liberté et l'équité des élections européennes ?

**La protection des élections européennes constitue un thème central dans le travail de toutes les instances et institutions de l'UE.**

À l'issue des élections européennes de 2019, la Commission européenne a analysé dans son rapport le déroulement des élections et en a déduit des besoins d'action. En vue d'adopter des mesures appropriées, **la Commission a présenté en 2020 un plan d'action pour la démocratie européenne. Dans ce cadre, de nombreuses initiatives ont été depuis mises en place afin de construire une démocratie plus résiliente et de renforcer la sécurité des élections.** Parmi les priorités de ce plan d'action figure entre autres la protection des démocraties européennes contre la désinformation et l'influence d'États étrangers dans l'espace informationnel. Dans cette optique, la Commission européenne a notamment soutenu la révision du code de conduite sur la lutte contre la désinformation. C'est sur la base de ce code que la Commission coopère avec des plateformes en ligne afin de faire front commun contre la désinformation.

**En décembre 2023, la Commission européenne a publié une recommandation relative à des processus électoraux inclusifs et résilients dans l'Union et à une meilleure garantie du bon déroulement des élections au Parlement européen.** Cette recommandation vise également la protection des élections contre les cybermenaces, la désinformation et les menaces hybrides en général. Dès novembre 2023, la Commission européenne a organisé un exercice commun des institutions européennes et des États membres de l'UE sur la cybersécurité en vue des prochaines élections au Parlement européen.

Depuis 2024, la présidence belge du Conseil de l'UE s'engage en faveur de la protection de la démocratie et de la promotion d'élections européennes libres et équitables. À cet égard, le groupe de travail du Conseil sur le renforcement de la résilience et la lutte contre les menaces hybrides revêt une importance particulière. Au sein de l'UE, ce groupe de travail endosse le rôle de coordinateur central afin de permettre une réaction conjointe de l'UEs face aux menaces hybrides telles que la désinformation. **Une étape essentielle dans l'amélioration de la capacité de réaction de l'UE face aux menaces hybrides et à la désinformation a résidé dans l'élaboration de deux « boîtes à outils »** : l'une destinée à la réaction aux menaces hybrides (boîte à outils hybride de l'UE), l'autre au traitement de la manipulation d'informations par des États étrangers et de l'ingérence dans l'espace informationnel (Foreign Information Manipulation and Interference (FIMI) Toolbox).

Les plateformes en ligne et les moteurs de recherche sont devenus des lieux importants pour le discours civique et la formation de l'opinion publique et du comportement électoral. **Le « Règlement sur les services numériques » (Digital Services Act ; DSA), entré en vigueur le 25 août 2023, oblige les très grandes plateformes et les très grands moteurs de recherche en ligne** à identifier, analyser et évaluer minutieusement tous les risques systémiques découlant de la conception et du fonctionnement de leurs services, y compris tout impact négatif, réel ou prévisible, sur le débat sociétal et les processus électoraux. Le DSA a conféré à la Commission européenne de larges compétences d'enquête et de surveillance, y compris la possibilité d'infliger des amendes. La Commission européenne a proposé un projet de lignes directrices destinées à aider les très grandes plateformes en ligne et les très grands moteurs de recherche à remplir leurs obligations en matière de réduction des risques systémiques auxquels sont exposés les processus d'élection.

## 10. Comment identifier les informations fausses et trompeuses et se protéger contre la désinformation ?

### a) Remettre en question au lieu de partager

Si des informations, images ou vidéos fausses ou trompeuses sont divulguées par des particuliers, ceux-ci ne le font souvent pas par malveillance. Mais dans le doute, de tels messages font cependant peur ou sèment la panique. Plus un message de ce type est émotionnel ou dramatique, plus il est partagé souvent. C'est pourquoi il est important de ne pas participer à ce phénomène et de garder son calme. Ne transmettez donc pas de contenus à d'autres sans les avoir vérifiés. Ne partagez pas de contenus qui vous paraissent douteux.

### b) Vérifier les sources et les expéditeurs du message

Il est toujours utile de comparer des informations douteuses avec au moins deux autres sources. L'actualité est reflétée par les offres médiatiques proposées par les chaînes d'information et les journaux et hebdomadaires. Consultez en outre les sites officiels des institutions ainsi que les canaux pertinents des institutions sur les réseaux sociaux. Vérifiez toujours qui a publié la vidéo, l'image ou l'information concernée. S'agit-il de l'auteur du matériel ou ce dernier a-t-il déjà été réacheminé plusieurs fois ? La mention d'un nom réel peut servir d'indice de l'authenticité d'un compte. De même, d'éventuelles informations fournies par les opérateurs des plateformes sur l'indépendance ou la proximité vis-à-vis du gouvernement de différents comptes peuvent être une aide à la décision. Sur les réseaux sociaux, limitez-vous aux comptes vérifiés des autorités et des institutions officielles. Sur les sites Internet, consultez les mentions légales. Celles-ci doivent indiquer le nom d'une personne responsable des contenus du site ainsi qu'une adresse complète, et pas uniquement, par exemple, une adresse électronique anonyme.

**c) Se servir des services de vérification des faits**

Un grand nombre de centres de recherche, d'organisations non gouvernementales et de médias indépendants examinent les informations et les affirmations qui circulent et les soumettent à une vérification afin de détecter les fausses informations et de les rectifier.

## 11. Où trouver plus d'informations ?

La responsable fédérale des élections présente des informations liées aux élections européennes :  
<https://www.bundeswahlleiterin.de/europawahlen/2024.html>.

La responsable fédérale des élections présente des faits contre la désinformation en relation avec les élections européennes :  
<https://www.bundeswahlleiterin.de/europawahlen/2024/fakten-desinformation.html>.

Le BMI fournit des informations détaillées sur les menaces hybrides :  
[www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html](http://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html).

Le BMI fournit de plus larges informations sur les différentes facettes de la désinformation en tant que menace hybride :  
<https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/artikel-desinformation-hybride-bedrohung.html>.

L'Office de presse et d'information du gouvernement fédéral (BPA) fournit, sur le site Internet du gouvernement fédéral, des informations sur le traitement de la désinformation :  
<https://www.bundesregierung.de/breg-de/themen/umgang-mit-desinformation>.

Le BPA attire l'attention sur l'augmentation des cas de désinformation et de deepfakes dans le cadre de la « super année électorale » 2024 : <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/desinformation-wahlen-2253208>.

Le BSI fournit diverses recommandations sur la sécurité de l'information :  
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Kandidierende.html>.

[https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html).

[https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/Identitaetsdiebstahl-Social-Media/identitaetsdiebstahl-social-media\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/Identitaetsdiebstahl-Social-Media/identitaetsdiebstahl-social-media_node.html).

[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html).

Le Parlement européen fournit des informations sur les élections européennes sur un site spécialement créé à cet effet : <https://elections.europa.eu/de/>.

**Informations éditoriales**

Éditeur

Ministère fédéral de l'Intérieur et du Territoire, 11014 Berlin

Internet : [www.bmi.bund.de](http://www.bmi.bund.de)

Édition

mars 2024

Numéro d'article : BMI24011

D'autres matériels d'information du gouvernement fédéral sont également disponibles par téléchargement ou par commande sur le site : [www.bundesregierung.de/publikationen](http://www.bundesregierung.de/publikationen)

Ce matériel d'information est publié par le gouvernement fédéral dans le cadre de son travail d'information. Le matériel d'information est délivré gratuitement et n'est pas destiné à la vente. Il ne doit être utilisé ni par les partis, ni par les candidats ou les militants durant une campagne électorale à des fins de publicité électorale. Cela vaut pour les élections du Bundestag, les élections au Landtag et les élections communales ainsi que pour les élections au Parlement européen.