Verbraucherzentrale
Rheinland-Pfalz

Cybercrime und Online-Abzocke

Politische Forderungen zur Landtagswahl 2026

1. Prävention und Aufklärung gegen Cyberkriminalität stärken

Forderung:

Die Landesregierung soll verstärkt in die Präventionsarbeit gegen Cyberkriminalität investieren – etwa durch Aufklärungskampagnen, die Einbindung in den Schulunterricht und öffentlichkeitswirksame Informationsangebote.

Begründung: Cyberkriminalität betrifft längst nicht mehr nur unerfahrene Nutzer:innen. Täter agieren hochprofessionell und sind oft international organisiert. Besonders verbreitet sind Phishing, Identitätsdiebstahl, Ransomware und manipulierte Anrufe im Namen seriöser Unternehmen. Die Folgen für Betroffene sind gravierend: Sie verlieren oft unwiederbringlich Geld, da Zahlungen ins Ausland gehen und kaum zurückverfolgt werden können. Gestohlene Daten werden für Einkäufe, Erpressung oder zur Verbreitung von Schadsoftware genutzt. Prävention durch Bildung und Aufklärung ist daher essenziell, um Verbraucher:innen zu schützen und ihre digitale Selbstverteidigung zu stärken.

---

2. Anbieteridentifikation und Transparenz im Netz verbessern

Forderung:

Webseitenanbieter sollen einer verpflichtenden Identifikationspflicht unterliegen, die wirksam überprüft wird.

Begründung: Viele Betrugsmaschen im Internet basieren auf der Täuschung durch scheinbar seriöse Webseiten. Eine verpflichtende und überprüfbare Anbieteridentifikation würde die Transparenz im Netz erhöhen und es Verbraucher:innen erleichtern, seriöse von unseriösen Angeboten zu unterscheiden. So kann Online-Abzocke frühzeitig erkannt und verhindert werden.

---

3. Sichere digitale Identitäten ermöglichen und schützen

Forderung:

Die Landesregierung dafür werben, dass Verbraucher:innen ihre digitale Identität sicher nachweisen können – z. B. durch Authentifizierung mittels ePerso und perspektivisch über die EU ID-Wallet.

Sichere digitale Identitäten sollen gezielt gefördert und implementiert werden.

Begründung: Die Einführung sicherer digitaler Identitäten ist entscheidend für den Schutz vor Cyberkriminalität. Zwei-Faktor-Authentifizierung und

verbraucherzentrale-rlp.de • E-Mail: info@vz-rlp.de • Telefon: 06131 28480
Für den Inhalt verantwortlich: Heike Troue, Vorständin

vertrauenswürdige Identitätsnachweise können verhindern, dass gestohlene Daten missbraucht werden.

Die EU ID-Wallet bietet hier eine zukunftsweisende Lösung, die Verbraucher:innen mehr Sicherheit und Kontrolle über ihre digitalen Daten gibt. Der Schutz der Nutzer:innen muss jetzt gestärkt werden, bevor zunehmend KI-generierte Betrugsmaschen noch mehr Verbraucher:innen schaden.

---

4. Strafverfolgung und Rechtsdurchsetzung bei Cybercrime ausbauen

Forderung:

Polizei und Staatsanwaltschaften müssen mit ausreichenden personellen und technischen Ressourcen ausgestattet werden, um Cyberkriminalität effektiv bekämpfen zu können.

Begründung: Die Täter agieren oft international und technisch versiert. Um Online-Abzocke konsequent zu verfolgen, braucht es spezialisierte Ermittlungsbehörden mit modernster Ausstattung und ausreichend Personal. Nur so kann die Rechtsdurchsetzung effektiv erfolgen und das Vertrauen der Verbraucher:innen in digitale Angebote gestärkt werden.

Rechtlicher Hintergrund:

Die EU NIS-2-Richtlinie verpflichtet Mitgliedstaaten zu stärkeren Maßnahmen gegen Cyberkriminalität, insbesondere gegenüber Unternehmen. Diese müssen künftig verbindliche Sicherheitsvorgaben einhalten und Meldepflichten erfüllen. Ab 2027 wird zudem eine Herstellerpflicht wirksam, Geräte mit besseren Schutzmechanismen wie Zwei-Faktor-Authentifizierung, Zero-Trust-Architekturen und nachhaltigen Updatepflichten auszustatten. Diese Maßnahmen sind wichtig – doch der Schutz der Verbraucher:innen muss schon jetzt beginnen.

verbraucherzentrale-rlp.de • E-Mail: info@vz-rlp.de • Telefon: 06131 28480
Für den Inhalt verantwortlich: Heike Troue, Vorständin