pcextreme

Abuse & acceptable use policy

PCextreme hanteert voor het gebruik van haar diensten een aantal gedragsregels. Deze gedragsregels hebben we vastgelegd in onze 'Acceptable Use Policy'. Overeenkomstig met onze Algemene Voorwaarden treden wij op tegen activiteiten die tegen deze regels ingaan.

Rapporteer misbruik

Om een melding van abuse (internetmisbruik) goed te kunnen onderzoeken, hebben wij alle informatie nodig die voorhanden is. Indien u de benodigde informatie verzameld hebt, kunt u de melding per e-mail toezenden aan abuse@pcextreme.nl

---

Definities

Spam: Ongevraagde, ongewenste of illegale e-mailberichten. **Spoofing:** Zich voordoen als iemand of iets. **Fraude:** Opzettelijke misleiding om op oneerlijke of onwettige wijze te profiteren **Phishing:** Een poging om gevoelige informatie te verwerven via elektronische communicatie door zich voor te doen als een betrouwbare entiteit. **DDOS:** Een type DOS-aanval waarbij meerdere geïnfecteerde systemen worden gebruikt om een Denial of Service-aanval (DoS) te veroorzaken op een systeem. **E-mail bombing:** Een vorm van internetmisbruik bestaande uit het verzenden van grote hoeveelheden e-mail naar een adres in een poging om de mailbox te laten overlopen of de server te overbelasten. **Flooding:** Een vorm van denial-of-service waarbij een aanvaller verzoeken verzendt naar een systeem in een poging om zoveel mogelijk servercapaciteit te verbruiken zodat het systeem niet meer kan reageren op legitiem verkeer. **Schadelijke software:** Ook bekend als malware, is software wat gedeeltelijk of volledige controle over uw computer geeft aan de maker van de malware. **Kwetsbaarheden:** Een zwakpunt waardoor een aanvaller de beveiliging van een systeem kan verminderen. **Hacken:** Proberen om toegang te verkrijgen tot computer- of netwerksystemen. **Exploiteren:** Het gebruik van een specifiek software onderdeel, gegevens of een reeks opdrachten die misbruik maken van een bug of

kwetsbaarheid om onbedoeld of onverwacht gedrag te veroorzaken op computersoftware, hardware of iets elektronischs (meestal geautomatiseerd).

---

1. Algemeen

1.1 Materiaal

Het is voor KLANT niet toegestaan enig materiaal te versturen of aan te bieden (via e-mail, website, uploaden of anderszins) dat inbreuk maakt op auteursrecht, handelsmerk, patent, handelsgeheim of andere eigendoms-rechten van een derde partij, inclusief, maar niet beperkt tot, het ongeoorloofd kopiëren van auteursrechtelijk beschermd materiaal, het digitaliseren en distribueren van fotomateriaal uit tijdschriften, boeken of andere auteursrechtelijk beschermde bronnen, en het ongeoorloofd verzenden van auteursrechtelijk beschermde software.

Het is voor KLANT niet toegestaan enig materiaal te versturen of aan te bieden (via e-mail, website, uploaden of anderszins) dat bedreigingen bevat of oproept tot lichamelijk geweld of het vernielen van eigendommen.

Het is voor KLANT niet toegestaan enig materiaal te versturen of aan te bieden (via e-mail, website, uploaden of anderszins) dat bij een andere Internet-gebruiker overlast veroorzaakt.

1.2 Privacy

Het is voor KLANT niet toegestaan doelbewust op zoek te gaan naar informatie over anderen, of bestanden, andere gegevens of wachtwoorden van anderen te kopiëren of te wijzigen, of zich voor te doen als een andere gebruiker, tenzij met uitdrukkelijke toestemming van die gebruiker.

Het is voor KLANT niet toegestaan inbreuk te maken op de privacy van individuele gebruikers door middel van het bekijken van hun e-mail of hun persoonlijke communicatie met andere gebruikers.

---

2. E-mail

2.1 Spam

Het is voor KLANT niet toegestaan ongevraagde commerciële e-mail (“UCE”) of ongevraagde bulk e-mail (“UBE”) te verzenden naar enige Internet-gebruiker via een PCEXTREME account of via enige andere netwerkverbinding die op enigerlei wijze PCEXTREME impliceert.

2.2 Mailinglists

Elke vorm van mailinglist-gebruik binnen het netwerk van PCEXTREME moet voldoen aan de richtlijnen van MAPS https://tools.ietf.org/html/rfc5782 en RFC 3098 http://www.faqs.org/rfcs/rfc3098.html. Wat onder andere, maar niet uitsluitend, inhoud dat de Internet-gebruiker zich middels een “Opt-in” en “Opt-out” moet kunnen in- en uitschrijven.

2.3 Header faking

Het is voor KLANT niet toegestaan de koppen van e-mail berichten te wijzigen met de bedoeling zijn of haar e-mail adres te verbergen.

Het is voor KLANT niet toegestaan te pogen zich als een ander voor te doen door gebruikmaking van vervalste headers of andere identificerende informatie.

2.4 Mailservers

Het is voor KLANT niet toegestaan tijdelijk of permanent een onvoldoende beveiligde mailserver aan het netwerk van PCEXTREME te koppelen. De mailserver van de KLANT moet begin- of eindstation voor e-mail zijn, geen tussenstation. PCEXTREME behoudt zich expliciet het recht voor een onvoldoende beveiligde mailserver zonder kennisgeving vooraf te blokkeren.

---

3. Website

3.1 Fraude

Het is voor KLANT niet toegestaan frauduleuze aanbiedingen te doen om producten, onderwerpen of diensten te kopen of te verkopen, of om enige vorm van financieel bedrog te promoten, zoals (maar niet beperkt tot) “piramide-systemen (Ponzi Scheming)”, “snel rijk worden-systemen” of “kettingbrieven”.

Het is voor KLANT niet toegestaan enige vorm van bedrieglijke online marketingpraktijken uit te voeren.

3.2 Privacy regels

Het is voor KLANT niet toegestaan persoonlijke gegevens van derden te verzamelen, of pogen te verzamelen, zonder hun medeweten of instemming (bijvoorbeeld, maar niet uitsluitend, in de vorm van “phishing”).

3.3 (Inter)nationale wet- en regelgeving

Het is voor KLANT niet toegestaan enig materiaal te aan te bieden dat, opzettelijk of niet, enige toepasselijke nationale of internationale wet, of enige regels die daaruit voortvloeien, overtreedt.

---

4. Server

4.1 Misbruik

Het is voor KLANT niet toegestaan diensten aan een gebruiker, systemen in een netwerk, netwerkdiensten of netwerkcommunicatie te verstoren, inclusief, maar niet beperkt tot, mailbombing, flooding, moedwillige pogingen een systeem te overbelasten, en broadcast-aanvallen.

Het is voor KLANT niet toegestaan virussen of andersoortige vormen van malicieuze programma’s in of buiten het netwerk van PCEXTREME of in het systeem te introduceren.

Het is voor KLANT niet toegestaan het systeem aan te wenden om zonder toestemming toegang te verkrijgen tot andere computersystemen, netwerken of programma’s.

4.2 Daemons

Het is voor KLANT niet toegestaan ongeoorloofde toegang te verkrijgen (of pogen te verkrijgen) tot systemen of netwerken, daaronder begrepen enige poging een systeem of een netwerk te proben, scannen of testen op kwetsbaarheden, of om beveiligings- of authenticatiemaatregelen te doorbreken zonder expliciete toestemming van de

eigenaar van het systeem of het netwerk.

Het is voor KLANT niet toegestaan zonder toestemming data of verkeer van enig netwerk of systeem te monitoren zonder expliciete toestemming van de eigenaar van het systeem of het netwerk.

Het is voor KLANT niet toegestaan inbreuk te maken op de integriteit van computer- en netwerksystemen; voorbeeld: klanten zullen niet opzettelijk programma's ontwikkelen of gebruiken die andere gebruikers hinderen of een computer, computersysteem of netwerk infiltreren en/of beschadigen of de softwarecomponenten van een computer, computersysteem of netwerk wijzigen.

4.3 Exploits

Het is voor KLANT niet toegestaan het systeem aan te wenden om zonder toestemming toegang te verkrijgen tot andere computersystemen, netwerken of programma's, al dan niet gebruik makend van bestaande lekken in programma's, computersystemen of netwerken.

4.4 Software

Het is voor KLANT niet toegestaan inbreuk te maken op wettelijke bescherming van auteursrecht of licentiering van programma's en gegevens.