Dark Web Monitoring *Terms of Service*

Overview Of Services

VIZST TECHNOLOGY Dark Web ID Monitoring Services are delivered as follows:

Un-managed:

- Monthly status report
- Alert emails sent to your own designated contact internally for any alerts detected
- Portal login

Managed:

- Monthly status report
- Alert emails sent to our IT Helpdesk with notification of alert overseen by VIZST TECHNOLOGY engineer
- Assistance in guidance on steps to take to mitigate risks from the alert
- Access to Technical Support inclusive in price.
- Client Portal

Each subscription includes 1x primary domain for monitoring. Additional domains that require monitoring have a 30% discount.

Dark Web Monitoring - Terms Of Service

Terms of Service & Monthly Service Cost:
The term of this service will be month to month but requires a sixty (60) day notice to cancel. Service will then cancel at the end of the month following 60 day notice. All services may be suspended at our discretion if invoices are over 30 days past due or at end of term. The monthly service cost will increase/decrease based on the number of products needed. Prices do not include tax.

Excluded Services:
Services rendered under this agreement include initial install/training. Further action to remove, change or correct Client passwords or other data is the responsibility of the Client. No other labour or support is implied or covered by this agreement. For support please refer to your support agreement with VIZST TECHNOLOGY. Where no Support agreement is in place our standard hourly rate will apply.

Limitation of Liability:
Client understands that no monitoring service or software product can fully protect them from digital theft. Vizst Technology Ltd HAS NO OTHER EXPRESS OR IMPLIED GUARANTEES, WARRANTIES OR CONDITIONS. Vizst Technology Ltd's LIABILITY FOR DIRECT OR INDIRECT DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT IS LIMITED TO THE AMOUNT PAID OR PAYABLE BY CLIENT TO Vizst Technology Ltd FOR THIS APPLICABLE PRODUCT/SERVICE FOR THE PAST SIX MONTHS. This agreement shall be governed by and construed in accordance with the laws of the United Kingdom.

Dark Web Monitoring FAQ's

What is Dark Web Monitoring?

The Dark Web is a hidden universe contained within the “Deep Web”- a sublayer of the Internet that is hidden from conventional search engines. Search engines like Google, BING and Yahoo only search .04% of the indexed or “surface” Internet. The other 99.96% of the Web consists of databases, private academic and government networks, and the Dark Web. The Dark Web is estimated at 550 times larger than the surface Web and growing. Because you can operate anonymously, the Dark Web holds a wealth of stolen data and illegal activity.

How Does Dark Web ID Monitoring Protection My Organisation?

Our service is designed to help both public and private sector organizations detect and mitigate cyber threats that leverage stolen email addresses and passwords. Dark Web ID leverages a combination of human and artificial intelligence that scours botnets, criminal chat rooms, blogs, Websites and bulletin boards, Peer to Peer networks, forums, private networks, and other blackmarket sites 24/7, 365 days a year to identify stolen credentials and other personally identifiable information (PII).

Data Source Locations, and Descriptions: Where Do We Find Data?

- Dark Web Chatroom: compromised data discovered in a hidden IRC;
- Hacking Site: compromised data exposed on a hacked Website or data dump site
- Hidden Theft Forum: compromised data published within a hacking forum community;
- P2P File Leak: compromised data leaked from a Peer-to-Peer file sharing program or network;
- Social Media Post: compromised data posted on a social media platform;
- C2 Server/Malware: compromised data harvested through botnets or on a command and control (C2) server.