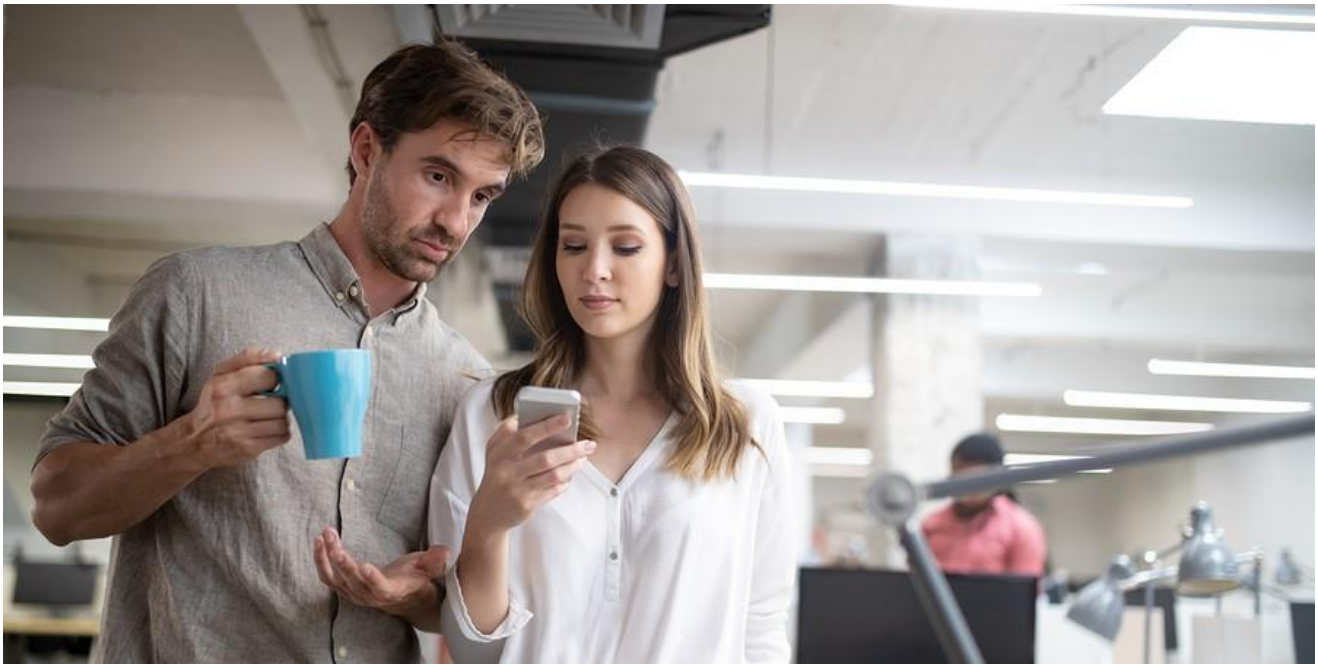
Internet Domain Name Provider, Network Solutions Data Breach Confirmed



eMazzanti Technologies reports on Network Solutions Data breach affecting millions of web.com domain name customers

Hoboken, New Jersey -- November 6, 2019 — eMazzanti Technologies, a NYC area IT security consultant and MSP, shares information on a data breach confirmed yesterday by Internet domain name provider, Network Solutions. eMazzanti believes it important to share this information broadly as organizations large and small may be significantly affected. Currently, eMazzanti helps business leaders deal with all types of evolving cyber-security threats.

Network Solutions, the company reporting the breach, is the world's first Internet domain name provider. It currently operates as a subsidiary of Web.com, the fourth largest domain name registrar with nearly seven million domains registered.

According to Web.com, hackers may have accessed as many as 22 million records belonging to past and present Network Solutions, Register.com and Web.com customers. The information possibly accessed includes name, address, phone number, and email address data and details regarding the services offered by the company to customers.

"Cyber vigilance from an experienced vendor is the best way to keep internal practices up to date and on the forefront of emerging technology designed to prevent a breach," stated Almi Dumi, CISO, eMazzanti Technologies. "Look for a firm credentialed with PCI QIR and CISSP qualifications that has

deep knowledge of hacker tactics and the dark web with comprehensive processes for preventive measures."

Network Solutions Data Breach Details

Network Solutions released this statement yesterday:

> **Important Security Information**
> November 5, 2019
>
> ### What Happened?
> On October 16, 2019, Network Solutions determined that a third-party gained unauthorized access to a limited number of our computer systems in late August 2019, and as a result, account information may have been accessed. No credit card data was compromised as a result of this incident.
>
> Upon discovery of this unauthorized access, the company immediately began working with an independent cybersecurity firm to conduct a comprehensive investigation to determine the scope of the incident, including the specific data impacted. We have also reported the intrusion to federal authorities and are notifying affected customers.
>
> Safeguarding our customers' information is core to our mission. We are committed to protecting our customers against misuse of their information and have invested heavily in cybersecurity. We will continue to do so as we incorporate the key learnings of this incident to further strengthen our cyber defenses.

What Information Was Involved?

Our investigation indicates that account information for current and former Network Solutions customers may have been accessed. This information includes contact details such as name, address, phone numbers, email address and information about the services that we offer to a given account holder. We encrypt credit card numbers and no credit card data was compromised as a result of this incident.

What Are We Doing?

Upon discovery, Network Solutions took immediate steps to stop the intrusion. We promptly engaged a leading independent cybersecurity firm to investigate and determine the scope of the incident. We notified the proper authorities and began working with federal law enforcement.

We are notifying affected customers through email and via our website, and as an additional precaution are requiring all users to reset their account passwords.

What You Can Do

We have taken additional steps to secure your account, and you will be required to reset your password the next time you log in to your Network Solutions account. As with any online service or platform, it is also good security practice to change your password often and use a unique password for each service.

Dark Web Search Services

Cyber-criminals use stolen passwords and other personal information to add credibility to scams and other threats. Personal data is usually purchased on the dark web from hackers who obtained them in recent security breaches.

> *If an individual's information has been stolen in a past breach, they may be more vulnerable to extortion and similar types of attack.*

eMazzanti Technologies offers services related to Dark Web identity protection. In addition to domain monitoring and thorough dark web searches, the company assists with remediation and improving its clients' security posture.

Avoid Becoming a Scam Victim

eMazzanti recommends these steps to avoid falling prey to extortion scams and other cyber-security threats:

- Check if personal information is for sale on the Dark Web from past breaches.
- Change passwords regularly.
- Use two-factor authentication.
- Cover computer camera and disable the microphone when not in use.
- Subscribe to security announcements.

Cyber-security Vigilance

Security awareness is the responsibility of everyone. Thus, in light of the Network Solutions data breach, eMazzanti urges business leaders to make this information available to ALL employees.

An organization's controls and cyber-security awareness should adapt to keep pace with quickly evolving cyber-security threats. Accordingly, anyone charged with data security who is unsure about what to do may call the IT security professionals at eMazzanti Technologies.