



Network Health Exposed to Sophisticated Email Phishing Attack

No financial information exposed; no evidence that exposed information misused in any way

MENASHA, WI – (Sept. 22, 2017) – In early August, two Network Health staff members were identified as the victims of a sophisticated email phishing attack by an unauthorized party which resulted in the potential exposure of their company emails. The emails did not contain any personal financial information and Network Health has no reason to believe that the exposed information was misused in any way.

Upon discovering the attack, Network Health took prompt action to secure the affected email accounts, to contain the impact and prevent further threats from the intruder. A forensic security expert was engaged to assess the attack and evaluate whether other areas of Network Health’s network were compromised. In addition, federal law enforcement officials were notified and are investigating the matter.

The information potentially exposed is primarily limited to member names and IDs, provider information, addresses, phone numbers and dates of birth. In limited circumstances, claims information and Health Insurance Claim Numbers may have been exposed. No credit card or financial information was exposed. Approximately 51,000 members whose information may have been accessed are being notified via letter.

Network Health maintains technical safeguards to protect against phishing incidents and detect intrusions. There are safeguards in place to ensure the privacy and security of all member information.

“We take the security and sensitive information of our members very seriously,” said Penny Ransom, Chief Administrative Officer of Network Health. “As a result of this attack, steps are underway to further improve the security of operations and prevent future incidents.”

These measures include enhanced organization wide re-education to recognize and report these more sophisticated phishing attempts, as well as a full review of security processes and procedures. In addition to notifying impacted individuals, Network Health has submitted notification of this incident to the Office for Civil Rights (OCR).

The 2017 U.S. State of Cybercrime survey reported phishing attacks have increased 10 percent since 2016. Last year alone, 1 in 131 emails are estimated to have contained malware, which is the highest rate in 5 years.

As a result of this exposure, Network Health is offering one year of free identity theft protection and monitoring to affected individuals. A dedicated call center has been established to answer any questions regarding the incident.

All questions should be directed to 855-609-5849.

###

About Network Health

Founded in 1982, Network Health offers customized commercial and Medicare health insurance services to employers, individuals and families in more than 23 counties throughout Wisconsin. Through its strong reputation for quality health care coverage and superior customer service, Network Health has grown to serve more than 134,000 members and 32,000 wellness participants. Learn more at networkhealth.com. Visit our blog at copilotwi.com.