



Chad Tester
COO

DOMINION VOICE AND DATA Shares 3 Best Practices for Thwarting Phishing Attacks

Leading Provider in Managed Technology Services Teaches Cyber Security Prevention Measures

MIDLOTHIAN, VA – December 2018 - Dominion Voice and Data, a leading managed technology services provider (MTSP), is helping small to mid-sized businesses (SMBs) thwart cyberattacks and protect their organizations from unnecessary downtime by addressing the most common tactic that cybercriminals use to attack modern workplaces; phishing. Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. According to PhishMe research, “91% of the time, phishing emails are behind successful cyberattacks.” Dominion Voice and Data is helping businesses identify the 3 tell-tale signs behind the majority of successful phishing attacks and how mere employee awareness can eliminate the vast majority of this threat from entering an organization.

“The overwhelming majority of security breaches caused by

phishing are completely avoidable,” stated Chad Tester, COO of Dominion Voice and Data. “While cybercriminals have grown more sophisticated in their approach, the average attack consists of the same key ingredients: an undereducated employee, effective bait and a temporary lapse in judgment. While we are in the business of securing an organization’s entire network and protecting them from any threats whatsoever, there are some initial steps that will safeguard a company without costing much time, energy or capital expenditure. These measures we’d like to share are extremely easy to implement and are excellent first steps in protecting a company from cybercrime.”

The first sign to look for is the sender’s name in the “From” field of the email. Cybercriminals often use misspelled email addresses, such as JohnnyStealyastuff@gmaail.com, for example, in order to deceive the receiver into thinking that the email is coming from a reputable company. At a quick glance, many recipients won’t recognize the typo in the address field and they’ll open

the email which opens them up to the bait.

The next step for employees is to hover their mouse over links, instead of clicking them without thinking about it. Lots of hackers use very long links or they hope that the recipient will just click on the link right away instead of previewing the destination by hovering above and making sure that the domains match where they expect to be directed. If the preview link looks suspicious, that’s probably because it isn’t a legitimate offer. We recommend deleting these types of emails.

The final step for employees is to look in the footer. One of the current laws around email marketing requires senders to leave a physical address within the footer of the email. This is often left-out by cybercriminals and is a very easy way to tell if the email is a phishing attempt. Furthermore, there should also be an “Unsubscribe” button at the bottom of the email, which is another step that most hackers ignore.

By simply addressing these three initial steps, SMBs can avoid the vast majority of cyberattacks coming at their business. They are some of the

simplest, yet most effective ways at minimizing risk within an organization. “If all organizations were even this educated about cyberattacks, we would see a dramatic drop in incidents,” concluded Tester.

ABOUT DOMINION VOICE AND DATA

Dominion Voice and Data is Central Virginia's Leading Business Phone Systems, Data Network Solutions, and Cloud-

Based Managed Services Company. Our mission is to advance our client’s business goals through delivery of superior technology solutions and world class support.

At Dominion, we are your trusted technology adviser and reliable business partner so that we can design you a solution that fits your business model.

Dominion Voice and Data is committed to maintaining the confidentiality of information that belong to our customers,

especially Protected Health Information. To that end, we adhere to the requirements of the HIPAA Privacy Rule and the HIPAA Security Rule. We comply with all Business Associate obligations under HIPAA/HITECH, enabling Dominion Voice and Data to provide the highest level of services to our customers involved in the healthcare professions.