

Identifying Phishing Emails

5 Ways You Can Spot a Dangerous Email Before It Is Too Late

Each year, the number of phishing attempts continues to grow, becoming more sophisticated and harmful as hackers get more creative in their attacks. The impact of a successful phishing attack can not only affect the victim, but can also be detrimental to a company's network, data and reputation. These emails often appear to be similar to other emails reaching your inbox, but have clearly identifiable signs that they could be spam and malicious.



#1 Incorrect Domain Name in Email Address

Hackers usually impersonate companies or well known institutions by using their domain name in the "From" section. However, if you look close enough, the email is completely different. Sometimes attackers use a non-descript email domain, something common enough that it *could* be associated with an organization.

Always double check the "mailed-by" and "signed-by" fields in an email. Emails from reputable companies will always have this information as a security check for their customers/recipients.



#2 Urgent or Threatening Language

Emails that insist immediate action must be taken or the loss of an opportunity is merely moments away are trying to create a sense of urgency, distracting targets from other red flags within the email.

#3 Suspicious Attachments or Incorrect Links

Many times hackers, in an attempt to mimic other emails within your inbox, will include attachments or links that may appear similar to others you regularly receive. For example, millions of people use the large file sharing platform, Dropbox, to send large files back and forth. It is common for hackers to disguise their Dropbox hyperlink with a malicious link instead of the correct access link.

#4 Misspelled Words or Grammatical Errors

Emails filled with typos, poor grammar, and mistakes that would not be easily made by large organizations are more likely to be fraudulent.

#5 Mismatched URLs

Oftentimes, hackers will hide malicious web domains in hyperlinked text. This is especially true for buttons or click-through aspects of emails. Rather than clicking on a link in an email that is not 100% trusted, hovering over the link first to look at it, can ensure a hidden malicious web domain is not clicked on.



How Arista Can Help

Arista's Cognitive Unified Edge (CUE) solutions help enable school IT administrators to monitor, protect and control their networks while also providing protection from evolving threats. CUE products provide enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

Santa Clara—Corporate Headquarters

5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500

Fax: +1-408-538-8920

Email: info@arista.com

Ireland—International Headquarters

3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office

9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office

Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office

9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989



Copyright © 2023 Arista Networks, Inc. All rights reserved. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. March 1, 2023