NORTH ATLANTIC NETWORKS

THE 10 THINGS YOU NEED TO KNOW ABOUT EMAIL SECURITY IN 2022

A NAN Specialty White Paper

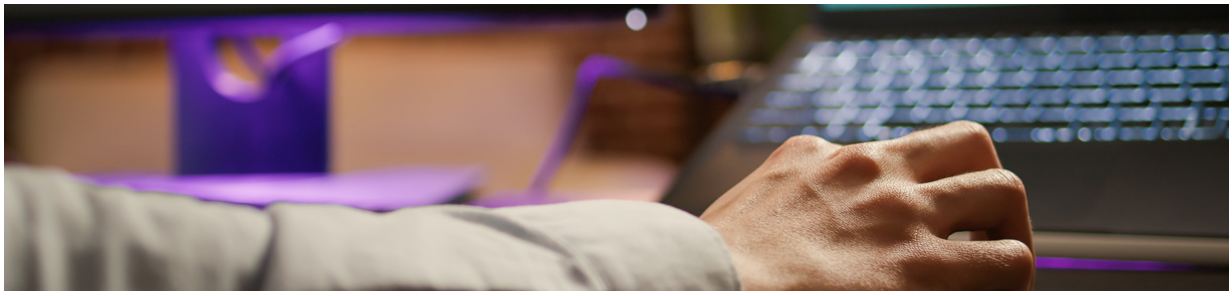
INTRODUCTION

Email has come a long way since the MIT program "MAILBOX", which was a program to leave messages on computers for other users, back in 1965. Now, approximately 319.6 billion emails were sent and received every day in 2021. Once email hosting websites aided the ease of use of this new medium, it completely revolutionized the world, especially in business. However, there is one drawback to this new mode of communication: it's really easy to hack.

The growth of cybercrime is so pervasive that the fallout cost is larger than country economies. In fact, it is estimated that the impact of cybercrime will reach $10.5 trillion by 2025. Email seems to be a large part of this foundation. According to a study by Mimecast, 1 in 50 emails contains some type of malicious content. And a data breach these days? They cost a business, on average, about $4.24 million.

In today's cyberthreat climate, every business must have proper "cyber hygiene" and that starts with email security policies. Educating and enforcing every employee on proper conduct around email and secure processes is the strongest foundation of a great defense. Read on to discover our ten high-security email practices to ward off threats.

1) EMAIL IS THE #1 THREAT VECTOR IN YOUR ATTACK SURFACE



It's easy for cybercriminals to make any email to any address appear as though it is coming from a source that the recipient may trust. Hackers can put anything they want in the "From" field. If your organization experiences a breach, it's more likely to come from an email source than anything else.

2) EMAIL SHOULD NEVER BE TRUSTED BY DEFAULT

If sensitive information is requested in an email, or anything about the message appears irregular, users should verify the credibility of the message through alternate channels outside of email. Instead, research and call the sender via telephone at their known number or phone number published on their website to verify that the communication was genuine. Never be afraid to verify – you are protecting yourself, your organization, the sender, and the sender's organization. When you receive similar calls to verify your emails, welcome them and thank the individual for their due diligence.

3) THE ROLE OF EMAIL IN BUSINESS HAS CHANGED

In today's cyber-threat landscape, email is best to be reserved for external communication for the purposes of paper trail, handoff, and documentation only. Email is no longer an optimal tool for secure collaboration or internal communication. Business class messaging tools such as Microsoft Teams or Slack should be used instead and email only when necessary.

4) IT'S NEVER SAFE TO SEND/STORE SENSITIVE INFORMATION IN YOUR EMAIL

Email inboxes are not secure repositories, nor are they designed to be. If transmitted to a recipient that is believed to be trusted, your information can still be at risk in an inbox outside of the organization that may be hacked later, already compromised, or, worse, both. Even if you have verified that you are speaking with the right person, never send sensitive information via email, not even to yourself. If an email is requesting sensitive information of any kind, do not trust it. No credible contact will ask you to submit any sensitive information via email including login credentials, credit card details, banking information, or other protected information.

5) ANYTHING IN YOUR INBOX CAN BE DANGEROUS

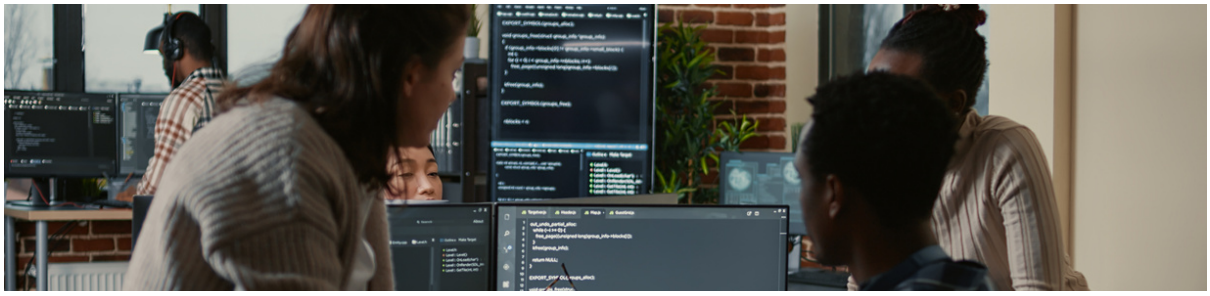
Yes. You read that correctly. Here are some inconvenient truths about our email inboxes:

- Just because an email says it has been scanned for Malware doesn't mean that it has been.
- Notices at the end of emails to delete if received by an unintended recipient are unenforceable.
- You can get hacked simply by opening an infected email even without opening attachments or clicking links. HTML Code and hidden files can be embedded in emails to infect your system the moment you open the message. If an email in your inbox appears "off" just don't open it. Contact your IT or security administrator for help.
- Links to "Unsubscribe" from pesky newsletters are never safe to click. They are a common attack vector because they are easily disguised as credible. Everyone loves the feeling of unsubscribing from junk email, and that's exactly why they work for hackers. Instead, mark the email as "Spam" and your email client and/or filtering service will forward future messages out of sight.
- Emails from trusted senders can be compromised (and potentially harmful to you) without the sender's knowledge. Once a user has been infected by malware or a hacker through email, the malicious software or actor's objective will be to spread as quickly as possible. This is often done by sending messages as the sender to the contacts that they communicate with most frequently. If you receive an email from a known contact, but you detect an unfamiliar communication style or formatting, contact the sender ASAP via phone.

6) ANTI MALWARE/VIRUS SOFTWARE DOES NOT BLOCK INFECTED EMAILS

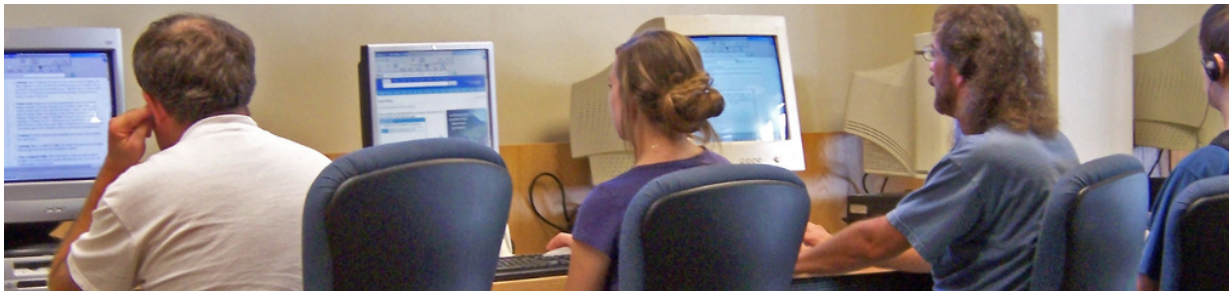
This is true even if you are using a desktop email client. To block potentially harmful email messages, you need a separate email filtering product such as Proofpoint. These products are effective at both incoming and outgoing filtering to protect your inbox from potential hackers and protect your contacts from harmful messages coming from your account if your email account has been compromised.

7) IN CASE OF FIRE: STOP, DROP, AND ROLL



Your organization needs a playbook for when suspicious attempts and email attacks occur. Common end-user questions are, “What do I do? Do I delete the email? Do I unplug my computer? Do I forward the email to my IT department?” In many cases, none of these things should be done right away. When your information security has been compromised, it is critical to act quickly and get an expert engaged. Your IT or information security administrator / partner can prevent it from spreading – therefore establishing open lines of communication to raise these alerts is key. To prepare, communicate what to do to your team in advance. Managed security providers can assist your team with training and enablement on best practices, as well as incentive programs for your users who properly classify fake spam emails.

8) NOT ALL EMAIL PLATFORMS ARE CREATED EQUAL



Always rely on business class email products, such as Office 365 or Exchange. Never use personal, consumer-grade email products for business email. Everything that exists in your inbox has been (effectively) given to the email company providing the service, therefore it is imperative to avoid consumer-grade products that lack the security and privacy policies that businesses depend on. Business-class email products offer and enable you to enforce critical security features such as Multi-Factor Authentication, forced password complexity and resetting policies, forced session timeout, data management and loss prevention policies, IP address and endpoint restrictions, and other critical tools essential for business communication. If you are using POP Email for your business, you should migrate to a modern platform with these capabilities ASAP. You must also ensure that the mail client used by your end users is up to date, fully patched, and configured securely. Your settings should block images by default and never download attachments automatically. This also goes for the browser(s) and operating system(s) in use by your organization.

9) MANAGED CYBERSECURITY / INFORMATION SECURITY PROVIDERS DIFFER WIDELY

When selecting a provider to help you achieve strength in cybersecurity – ensure that they are credible, capable, and are leveraging a cutting-edge tech stack that ranks highly in detection during independent, third-party studies. Specifically request information on their change management process, remediation

practices, incident response protocol, and the technical certifications of the resources who will be responsible for managing your equipment and enforcing your policies. Do not be afraid to ask them if any of their customers have experienced a major information security breach. If you are subject to regulation and compliance, make sure that the partner that you select can educate you on the technical and business requirements of maintaining and demonstrating compliance to your regulators. Don't take their word on their expertise and ability to deliver – instead, ask some of their customers about the experience of working with that provider.

10) WE ARE ALL IN THIS TOGETHER

Email cybercriminals and threat-actors do not discriminate against businesses of any type or size. We are all responsible for keeping each other safe. Organizations should adopt supportive and encouraging cybersecurity practices that feature routine training and enablement. If a breach of security occurs, treating it as a learning opportunity (vs. finger pointing and corrective action) is most productive in establishing a proactive security posture.

KEY TAKEAWAYS

1

Email is the most common attack vector for cybercriminal attacks.

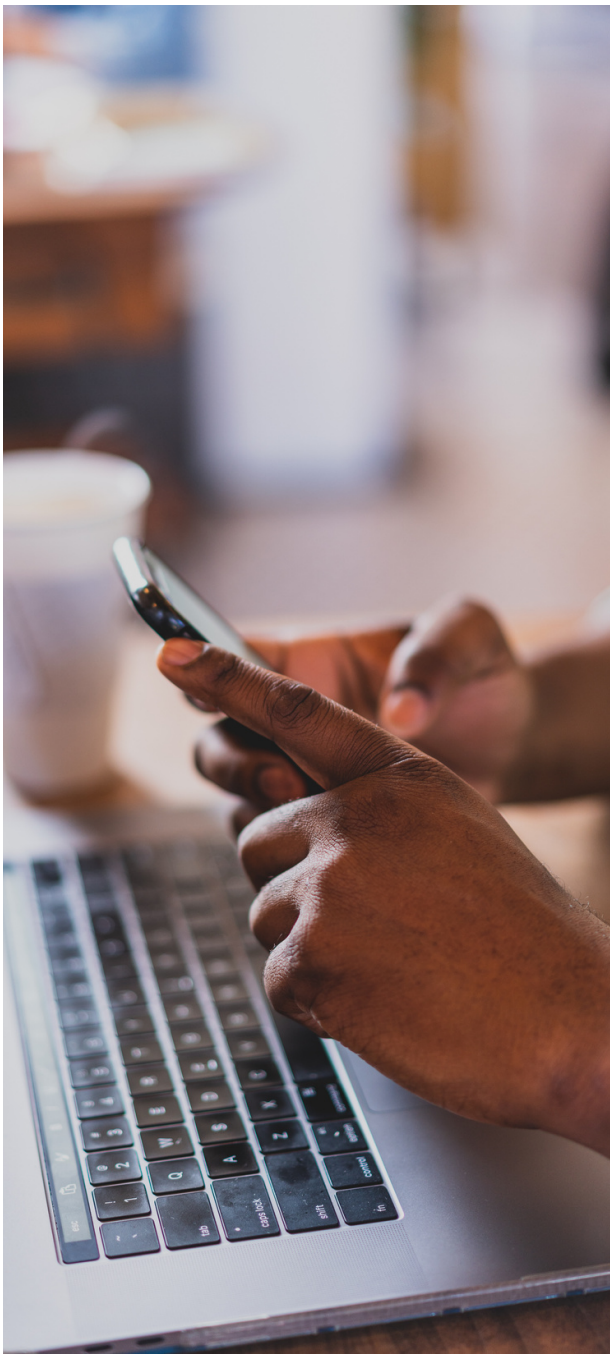
2

It is not safe to store or transmit any sensitive data using email.

3

Educate your teams on how to react using best practices and enablement.

ABOUT NAN



For over 25 years, North Atlantic Networks (NAN) has been the preeminent information and network security partner for the world's most regulated industries, Fortune 500 companies, state and federal government agencies, biopharma, financial institutions, and major retailers.

If you have experienced an information security event and need remediation assistance, or would like a no-cost cybersecurity assessment, please feel free to contact us anytime at info@nan.com or 800-299-3330

NORTH ATLANTIC NETWORKS
16 MASON AVENUE, NORTH ATTLEBORO, MA 02760
WWW.NAN.COM | 1-800-299-3330