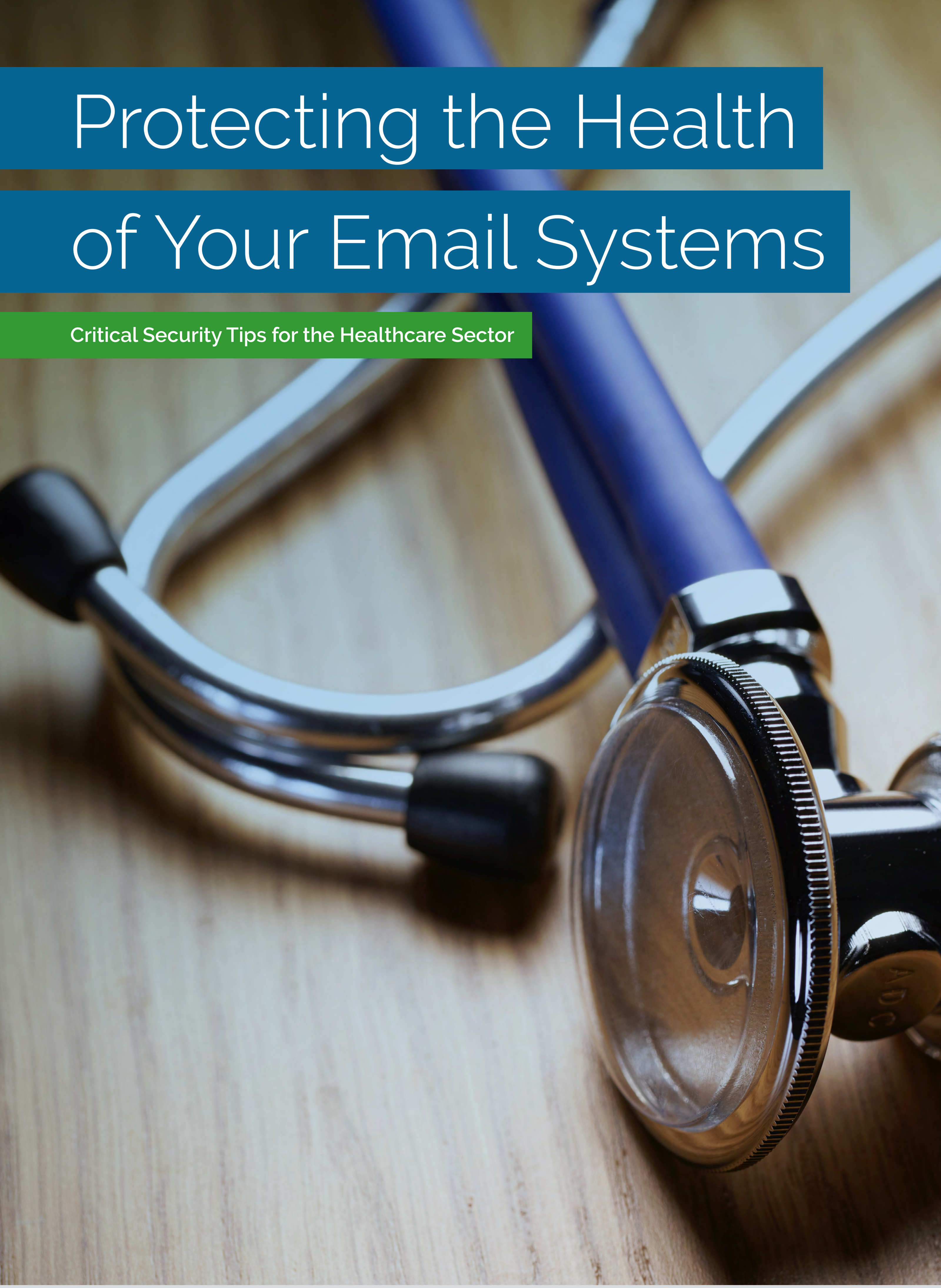
Protecting the Health of Your Email Systems

Critical Security Tips for the Healthcare Sector



MDaemon® technologies

Whether you run a multi-campus medical center or a small private practice, you've likely heard about cybercriminals who try to trick you and your employees into clicking a link or downloading an attachment so they can steal your organization's money or protected data. This is called phishing, and it's just one of the email security attacks that healthcare organizations are facing now more than ever.

Since the beginning of 2020, healthcare-related phishing targets have included hospitals, research laboratories, healthcare providers and pharmaceutical companies. This list is nowhere near complete, but to cite just a few examples:

- An employee of Houston-based Legacy Community Health Services responded to a phishing email that allowed unauthorized access to thousands of patients' information.
- Magellan Health and eight of its entities reported email hacking incidents affecting 364,892 individuals' health information due to a ransomware attack. The hacker got in through a phishing email by impersonating a client and accessed a corporate server that stored personal information including names, Social Security numbers, health insurance account information, tax details and addresses of clients.
- The Central California Alliance for Health, a nonprofit Medicaid health plan, notified 35,883 members of an employee email hacking incident that exposed their information.
- Earlier in the year, the Department of Health and Human Services reported that it is under attack on a daily basis.
- Looking through the latest Health IT Security monthly news archive turns up many examples of phishing, ransomware, malware, spoofing, password theft and other data leaks, and server vulnerabilities that affect millions of patients and financial donors.
- In July, authorities in the U.S., U.K. and Canada all issued warnings about serious cyberattacks against healthcare organizations and others involved in the coronavirus response. The purpose of these attacks? Theft of intellectual property during the race to develop a vaccine. The tool of choice? Spear-phishing email attacks.

Even if you weren't fully aware of these risks before the COVID-19 pandemic, it's crucial that you are now. These cybercriminals are exploiting widespread fear and uncertainty to target healthcare organizations of all kinds and are setting their malware to launch more quickly once inside healthcare IT networks, according to the Wall Street Journal. The losses can be staggering, affecting millions of patients and costing millions of dollars.

Why All the Email Attacks?

There's an additional complication in 2020: Like other businesses around the world, healthcare facilities are increasingly at risk due to the large numbers of employees accessing protected networks from home. If any point within your network becomes compromised by a successful phishing email, the attacker can gain access to a legitimate email address from which to launch other attacks. The imposter can then lie in wait, scanning email messages for details around financial transactions or patient data, then stage a full-blown attack when sufficient information or access has been gathered.

The phishing industry is so lucrative for scammers because the barriers to entry are low relative to potential huge payouts. With botnets-for-hire and Malware as a Service (MaaS), cybercriminals have an aggressive arsenal of tools at their disposal to propagate their campaigns. No healthcare facility is too big or too small to fall victim to email-borne scams. In fact, cybercriminals often target smaller organizations based on the assumption that smaller companies are less likely to have the latest security systems in place.

Against this onslaught, your healthcare organization has two major lines of defense:

- Fully educating all of your network users against email scams including phishing.
- Layered security strategies that maximize email security and block attacks before they reach your users.

Targeting the Big Platforms

In August 2019, Threatpost reported on what was then a new type of spear-phishing attack that was able to evade the security of Microsoft Exchange Online Protection. Sent via Google Drive, the deceptive email claims to be from the CEO of your organization including key information about the company to avoid suspicion by recipients. Because the email is sent by an authentic service, it's able to bypass Microsoft Exchange Online Protection on its way to users' inboxes.

The point is, Microsoft's built-in security features are not enough to protect your organization against these type of highly targeted spear-phishing attacks, particularly since cybercriminals are focused on ways to evade these protections. Just like in your home, installing layers of security is always more effective. You don't just lock your doors; an alarm system, motion-triggered lights and outdoor cameras all do their part to keep the bad guys away. And you can do the same thing within your email security.

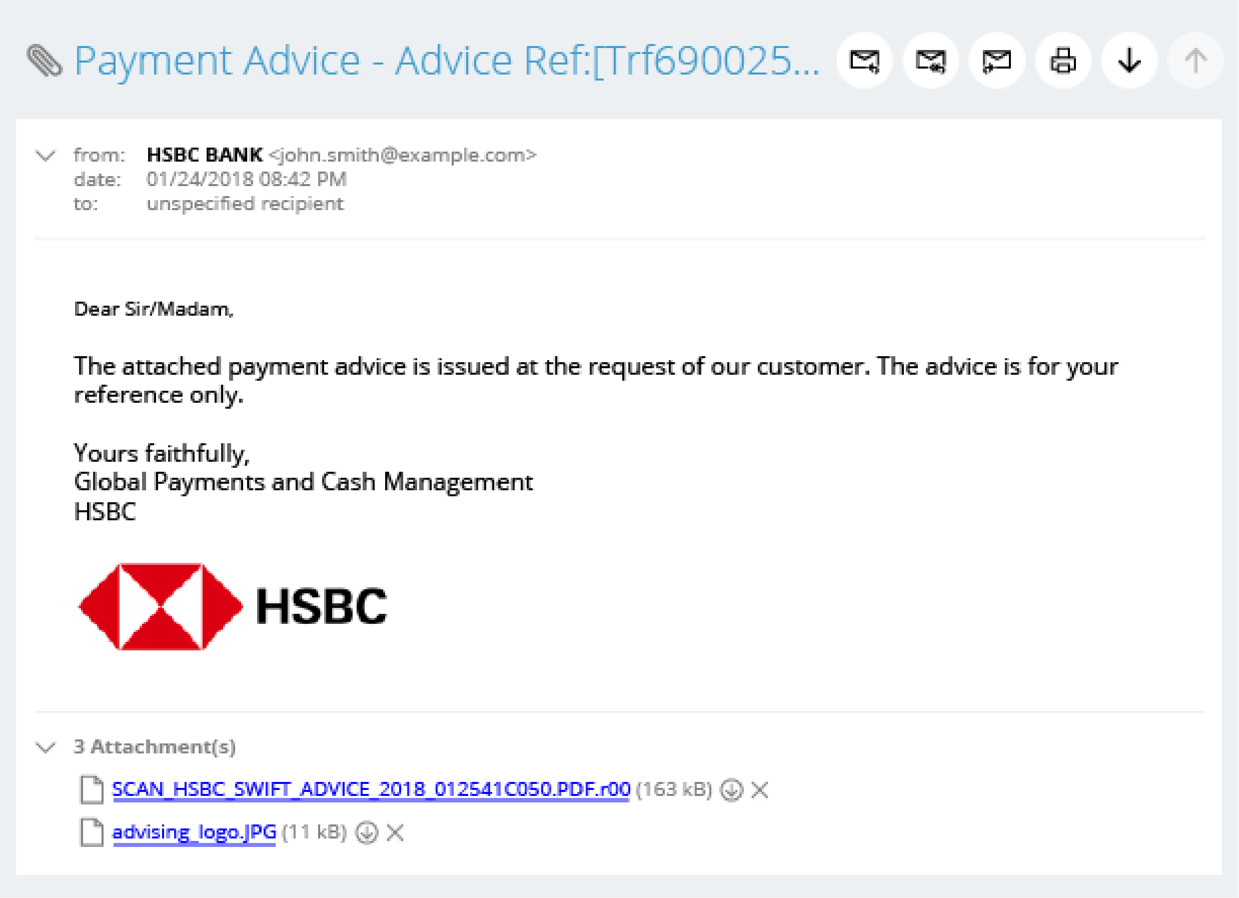
No Spam Filter or Email Gateway Can Block 100% of All Spam

Spam filters and email gateways have proven quite effective at blocking most of the junk email sent by the thousands on a daily basis, but cybercriminals are always looking for new ways to bypass security measures through social engineering, new strains of malware, and exploiting newly discovered security flaws in Microsoft Exchange Server and cloud email platforms. That's why user training must always be a top priority for all healthcare organizations that use email.

Employee Education

Here are our top tips on how to identify and protect your organization from phishing attacks. Make your employees aware of all of them, and reinforce this information with user training and anti-phishing drills whenever possible.

1. Watch out for messages disguised as something expected, like a shipment or payment notification. These often contain links to malware sites. Here's an example using a phishing email we received claiming to come from HSBC.



Payment Advice - Advice Ref:[Trf690025...

from: **HSBC BANK** <john.smith@example.com>
date: 01/24/2018 08:42 PM
to: unspecified recipient

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

3 Attachment(s)

SCAN_HSBC_SWIFT_ADVICE_2018_012541C050.PDF.r00 (163 kB)
advising_logo.JPG (11 kB)

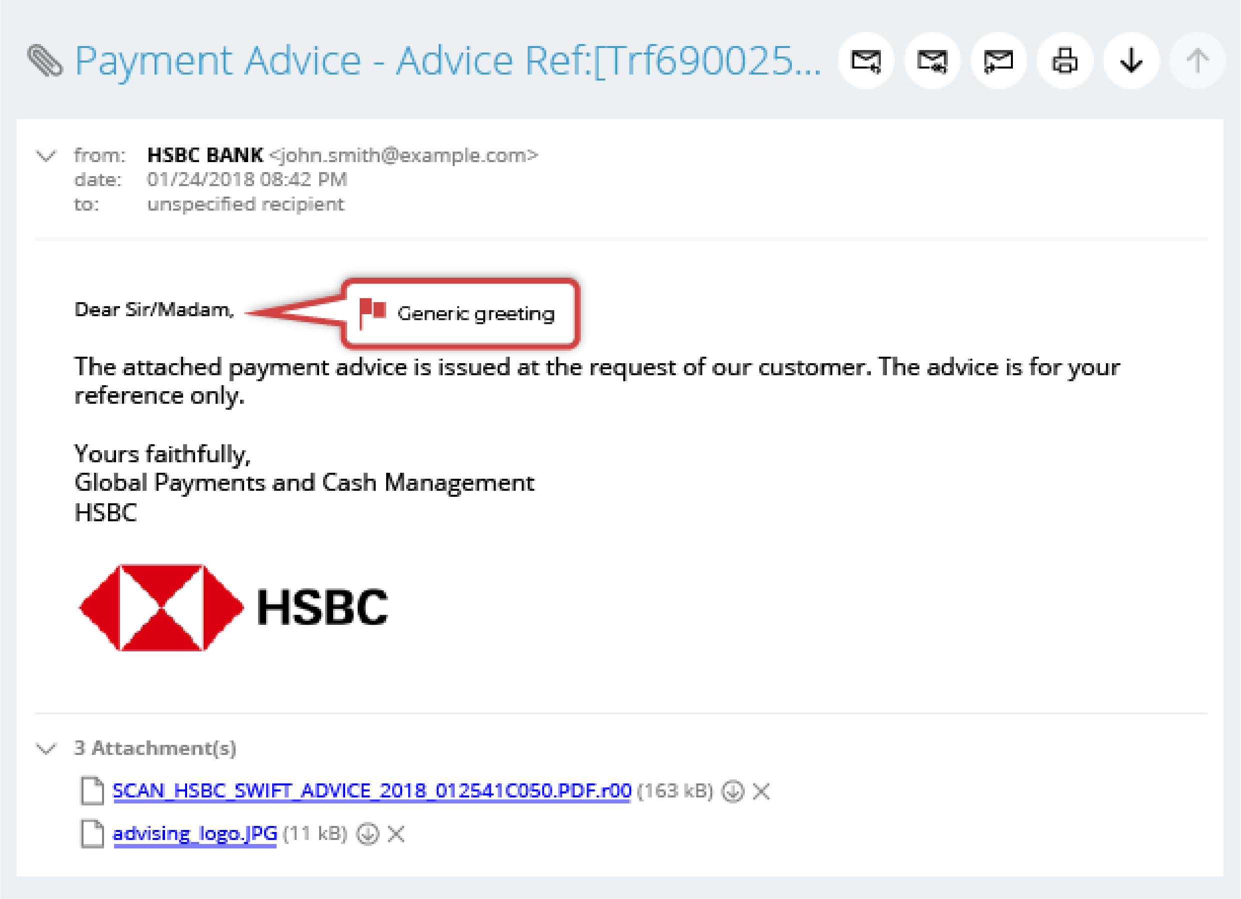
2. Watch for messages asking for personal information such as account numbers, Social Security numbers, and other personal information, as legitimate companies will never ask for this information over email. (Security Gateway for Email's Data Leak Prevention rules also prevent this type of data from being sent; see the section on Your Electronic Defenses within this ebook and check out this video.)

3. Beware of urgent or threatening messages claiming that your account has been suspended and prompting you to click on a link to unlock your account.

4. Check for poor grammar or spelling errors. While legitimate companies are very strict about emails they send out, phishing emails often contain poor spelling or grammar.

5. Don't trust the URL you see! Always hover your mouse over the link to view its real destination. Even if the link claims to point to a known, reputable site, it's always safer to manually type the URL into your browser's address bar.

6. Check the greeting – Is the message addressed to a generic recipient, such as "Valued customer" or "Sir/Madam?" If so, think twice! Legitimate businesses know and will often use your real first and last name. In our HSBC example, notice the generic greeting.



Payment Advice - Advice Ref:[Trf690025...

from: **HSBC BANK** <john.smith@example.com>
date: 01/24/2018 08:42 PM
to: unspecified recipient

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

3 Attachment(s)

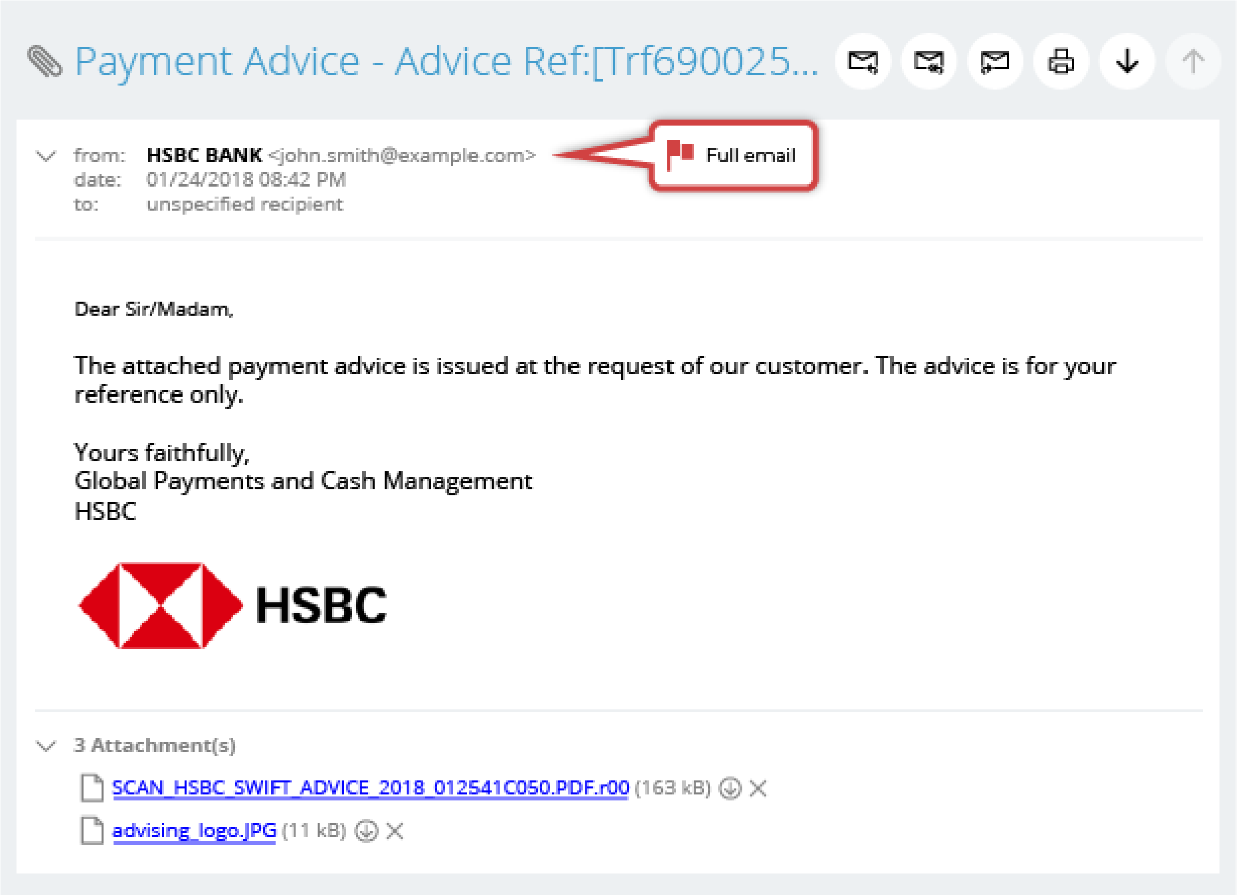
SCAN_HSBC_SWIFT_ADVICE_2018_012541C050.PDF.r00 (163 kB)
advising_logo.JPG (11 kB)

7. Check the signature block – In addition to the greeting, phishing emails often leave out important information in the signature. Legitimate businesses will always have accurate contact details in their signature block, so if a message's signature looks incomplete or inaccurate, chances are it's spam. In our HSBC example, the sender's name and contact information are missing from the signature.

8. Don't download unverified or unexpected attachments – With the proliferation of Ransomware as a Service (RaaS), cybercriminals have an easy mechanism for distributing malware-laden spam messages to thousands of users. Because the payout for ransomware can be quite high, even one successful ransomware infection could net the spammer large amounts of money. If there's ANY doubt about the identity of the message sender or the contents of an attachment, play it safe and don't download the attachment.

9. Don't trust the "From" address – Many phishing emails will have a forged sender address. Note this address is displayed in two places: The Envelope From is used by mail servers to generate NDR (non delivery report or "bounced") messages, while the Header From is used by the email client to display information in the "From" field. Both of these headers can be spoofed.

MDaemon Webmail has built-in security features to help users easily identify spoofed emails, those emails that seek to disguise an unknown sender. For instance, many mail clients hide the From address, only showing the From name, which can be easily spoofed. In MDaemon Webmail, the From address is always displayed, giving users a clearer view into the sender's email address and helping them identify spoofed senders. Using our HSBC example, the actual sender is highlighted.



Payment Advice - Advice Ref:[Trf690025...

from: HSBC BANK <john.smith@example.com>
date: 01/24/2018 08:42 PM
to: unspecified recipient

Full email

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

HSBC

3 Attachment(s)

SCAN_HSBC_SWIFT_ADVICE_2018_012541C050.PDF.r00 (163 kB)

advising_logo.JPG (11 kB)

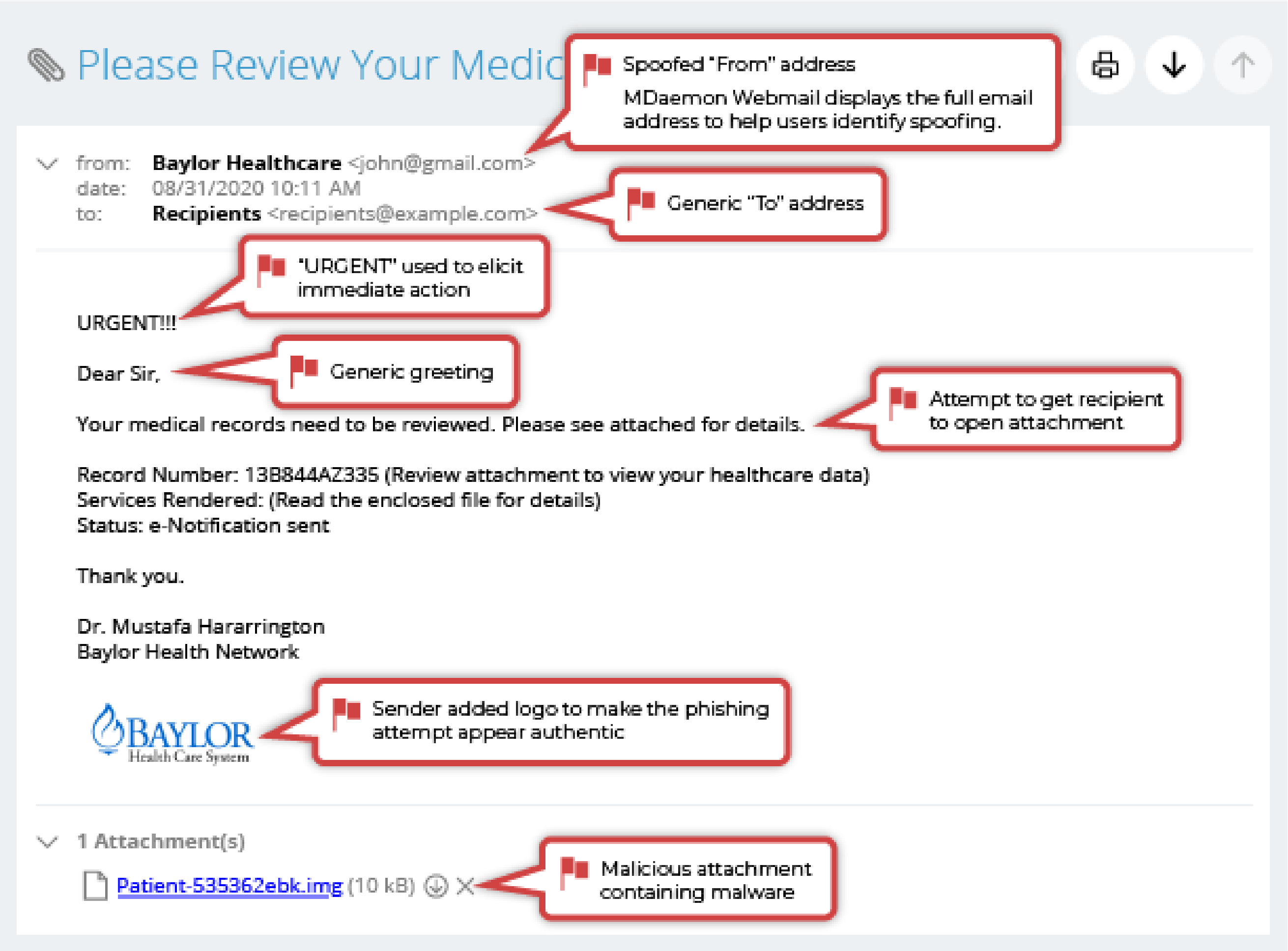
10. Don't enable macros – While we're on the subject of ransomware, another common entry point for ransomware infections is through macros in Microsoft Word documents. These documents often arrive in phishing emails claiming to have important content from HR, finance, or another important department; to trick the user, they ask the user to enable macros. Never trust an email that asks you to enable macros within a Word document. If you'd prefer your users never even see such emails, Security Gateway for Email detects Word documents with macros and prevents them from being delivered.

What a Healthcare Phishing Attack Looks Like

This example was scanned by the MDaemon Email Server, determined to be spam, and placed in the spam folder for review (although MDaemon can also be configured to delete spam instead of placing it in the user's spam folder).

In this example, the scammer has used display name spoofing to make the message appear to be from Baylor Healthcare (recently renamed Baylor Scott & White). Most large healthcare organizations have policies regarding privacy and email communications. You can read Baylor Scott & White's privacy policy here on their website. But for most of us who remain unaware of Baylor's policies, it's important to know what to look for to avoid becoming the next victim of phishing scams.

Using this healthcare example, here are the items to look out for when reviewing a suspicious email.



Please Review Your Medic

from: **Baylor Healthcare** <john@gmail.com>
date: 08/31/2020 10:11 AM
to: **Recipients** <recipients@example.com>

URGENT!!!

Dear Sir,

Your medical records need to be reviewed. Please see attached for details.

Record Number: 13B844AZ335 (Review attachment to view your healthcare data)
Services Rendered: (Read the enclosed file for details)
Status: e-Notification sent

Thank you.

Dr. Mustafa Hararrington
Baylor Health Network

1 Attachment(s)
Patient-535362ebk.img (10 kB)

Spoofed "From" address
MDaemon Webmail displays the full email address to help users identify spoofing.

Generic "To" address

"URGENT" used to elicit immediate action

Generic greeting

Attempt to get recipient to open attachment

Sender added logo to make the phishing attempt appear authentic

Malicious attachment containing malware

While these tips cover common phishing attacks, cybercriminals are constantly evolving their tactics to be more effective. One recently developed attack involves sending heavily researched and carefully crafted messages that may contain no malware or spam-like characteristics.

Business Email Compromise (BEC) Email Attacks

Referred to as the “Billion Dollar Scam” by the Federal Bureau of Investigation, a very specific type of scam known as the Business Email Compromise (BEC) generates around $301 million every month, or $3.6 billion every year, according to a 2019 report by the Financial Crimes Enforcement Network. In 2020, threat actors have been leveraging widespread fears about the coronavirus pandemic by impersonating reputable institutions like the World Health Organization and the Centers for Disease Control or by enticing recipients with plausible claims about healthcare treatments, informational webinars, bonuses for working through the pandemic, etc.

Hospitals and other healthcare facilities must be aware of the BEC scam, which has many variations and could result in substantial loss of money, data security, or goods such as prescription drugs.

Four Reasons BEC Scams Work So Well

So what makes a BEC attack so dangerous, and so effective?

1. **BEC Scams Are Highly Targeted**

   These scammers aren’t blasting thousands of the same email. They’ve done the research, using publicly available information on sites such as LinkedIn, Facebook and even the website of the healthcare organization, to gain insight into the company’s business practices. They will often study the writing styles of the executive team, which allows the scammers to craft convincing emails. They sidestep basic security strategies such as email filtering by finding only the most appropriate targets and grooming them by sending multiple conversational emails. These emails appear sophisticated and look legitimate, sometimes tricking even the most careful user.

2. **They Contain No Malware**

   Unlike the old style of phishing where users are told to click on a link, BEC emails have no suspicious inks. This means they can sometimes evade spam filters, and the target doesn’t see any red flags.

3. **They Exploit Human Nature**

   BEC emails carefully impersonate an actual person, complete with authentic-looking email addresses, formatting, company names, and titles. The target may have unknowingly been emailing back and forth with the scammer and comes to trust they are who they claim to be. So when asked to send bank information, for example, the target assumes the request is authentic and complies.

4. **They Are Often Under-reported**

   The targets of BEC scams often don’t realize they made a mistake until much later. Even upon realization, many companies don’t report the incident for fear of damaging their reputation with their customers. Not reporting such incidents allows perpetrators to simply move on to their next victim.

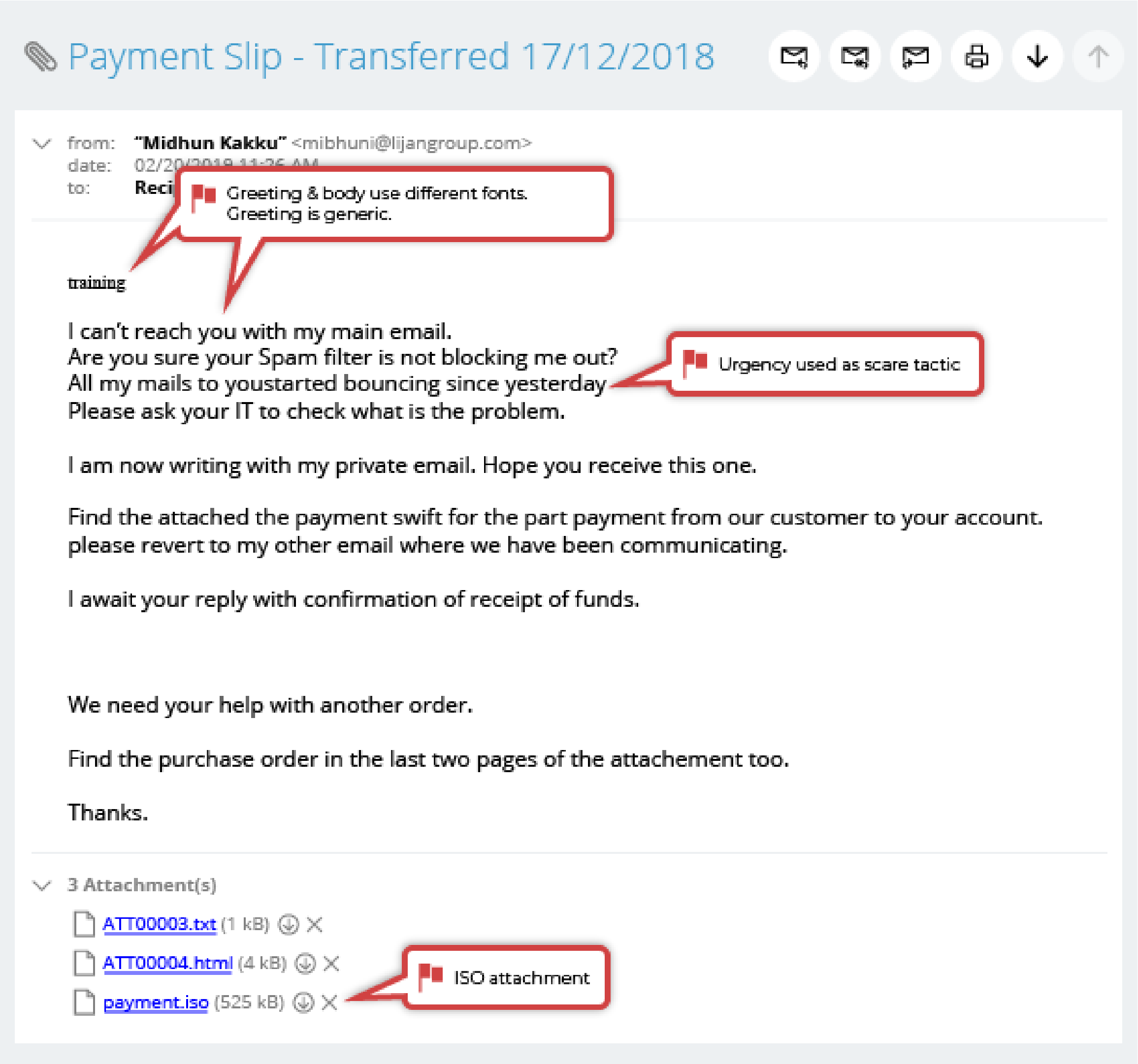
Defending Against BEC Attacks

Because BEC attacks are often so well-crafted and contain no malware or other malicious attachments, they are able to bypass standard security measures; therefore, the most critical part of stopping BEC attacks is user awareness and education. These tips should help your employees identify a BEC attempt if one should slip through your spam filter or email gateway.

- Double-check the sender email address and know how to recognize spoofing and other impersonation tactics. MDaemon Webmail displays the full email header to help users identify spoofed emails. (See page 7 for example.)
- Don't overshare on your own social media.
- Don't open email from unknown sources.
- Verify all wire transfer requests via phone or face-to-face.
- Know customers' and vendors' business practices.
- Run antivirus software often.
- Use two-factor authentication.
- Forward, don't reply; this ensures you manually enter the appropriate email address.

What a BEC Attack Looks Like

Here's an example where the scammer is using a classic BEC attack to try to get the recipient to open a malicious ISO file.



Payment Slip - Transferred 17/12/2018

from: "Midhun Kakku" <mibhuni@lijangroup.com>
date: 02/20/2019 11:26 AM
to: Reci

Greeting & body use different fonts.
Greeting is generic.

training

I can't reach you with my main email.
Are you sure your Spam filter is not blocking me out?
All my mails to youstarted bouncing since yesterday
Please ask your IT to check what is the problem.

Urgency used as scare tactic

I am now writing with my private email. Hope you receive this one.

Find the attached the payment swift for the part payment from our customer to your account.
please revert to my other email where we have been communicating.

I await your reply with confirmation of receipt of funds.

We need your help with another order.

Find the purchase order in the last two pages of the attachement too.

Thanks.

3 Attachment(s)

ATT00003.txt (1 kB)
ATT00004.html (4 kB)
payment.iso (525 kB)

ISO attachment

Your Electronic Defenses

Clearly, no one wants to be the healthcare organization that has to notify its patients of a data breach. But your organization's first line of defense doesn't have to rely on humans; how much spam your employees receive can minimize your risk of attack and keep your organization from being a victim of cybercrime.

If an email security company or hosted provider tells you their spam filter will catch 100% of spam, they're not being completely honest. Most companies specify their products will catch 99% or 99.5% in their SLA (Service Level Agreement), with a false-positive rate of %.0001 or less. That's reasonable and to be expected, especially considering the statistics.

According to public data, spam made up more than 29% of global email traffic in 2019. Considering that an estimated 306 billion email messages are being sent per day worldwide in 2020, that's almost 89 million spam messages sent every day. In addition, spam is becoming more dangerous, with cryptojacking overtaking ransomware as the attack vector of choice for cybercriminals, and malware-as-a service making cybercrime more attractive for bad actors.

At MDaemon Technologies, we have been a pioneer in email and security technology for over two decades. We developed the MDaemon email server and Security Gateway for Email to protect your users from spam, malware, phishing attempts, and all of the other junk that often floods your organization's inboxes. Here are the steps you can take to tighten up your email security against these threats.

- Enable reverse lookups to verify the legitimacy of the sender.
- Use the antivirus features in MDaemon and Security Gateway to scan all inbound and outbound email traffic.
- Configure your email server to block connections from local clients that are not using SMTP authentication to validate the identity of the sender.
- Use the latest technologies to secure your domain against spoofing and message tampering, including SPF (to help against spoofing), DKIM (to validate message authenticity and protect against message tampering) & DMARC (to allow domain owners to set policies on how suspicious messages from their domain should be handled).
- Require two-factor authentication.
- Require strong passwords and force changes periodically.
- Provide regular end-user training on all scam formats including BEC.
- Use message notification features to identify when an email comes from an external source.
- Secure your domain against lookalike domain spam by registering similar domains.
- Don't allow the mail server or gateway to trust messages from unknown sources.
- Establish strict processes for wire transfers.

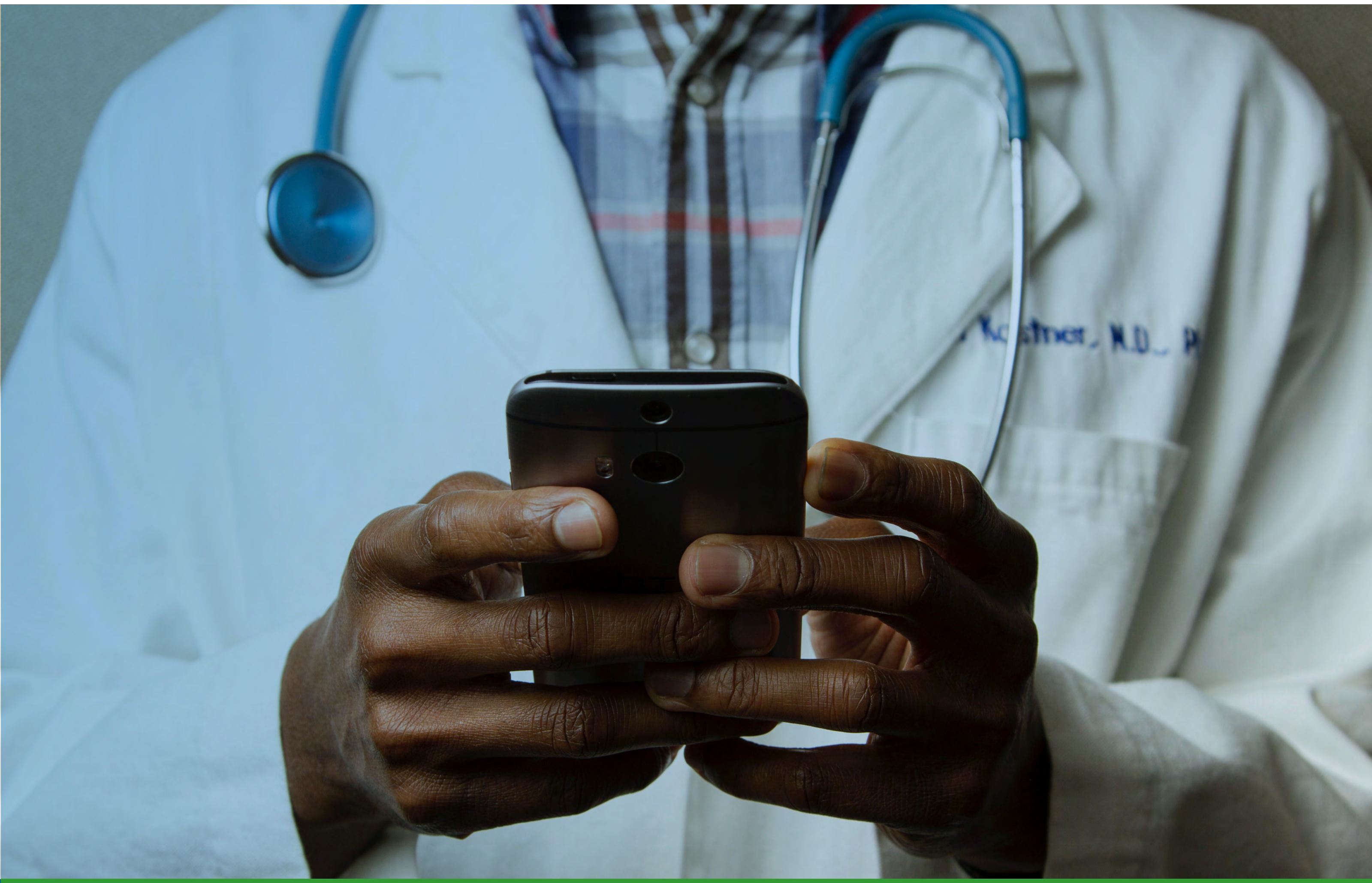
In addition, be sure to focus on outbound email threats to your healthcare organization. The MDaemon Security Gateway includes more than 70 data leak prevention (DLP) rules that help prevent unauthorized transmission of sensitive information such as personal identification numbers, credit card numbers, and other types of confidential data. These rules can be configured to send messages containing sensitive content to administrative quarantine for further review, redirect the message to a designated address, or encrypt the message. We recommend enabling the appropriate DLP rules to align with the security policies of your organization.

Ensuring the Health of Your Email Security

If there's email, there will always be cybercriminals focused on using the platform to attack your organization. As the IT professional responsible for the email security for a healthcare organization, your job is made much easier by implementing the software, tools and education that MDaemon Technologies provides.

The MDaemon Email Server and Security Gateway for Email Servers are trusted by IT professionals around the world. They include a variety of features to protect your healthcare facility from spam, malware and leaks of sensitive business data – and at a price that can often save you time and money.

Would you like to learn more about how MDaemon Technologies' Security Gateway for Email can help protect your healthcare facility and its data? Visit our Email Security for Healthcare Organizations page to sign up for hosted or on-premise email protection.



SecurityGateway for Healthcare Organizations