Email security

Did you know your email signature could be a security weak point?

breathetechnology

support | cloud | security | infrastructure | comms

EMPOWERING YOU THROUGH SECURE TECHNOLOGY

You're managing your responsibilities, and your day starts like any other. You check your email and find an urgent request from a key contact. It has their usual email signature at the bottom.

You follow their instructions… only to realise later that the email was a sophisticated scam. The email signature, so familiar and seemingly reliable, was expertly forged. The damage is done, and you're left wondering how you could have been so easily deceived.

This scenario is a growing reality for many organisations. Email signatures can be a gateway for cyber criminals to exploit personal and corporate vulnerabilities. While we carefully create these signatures to reflect our professionalism, we rarely consider their security implications.

Email signatures can include names, titles, contact information, and sometimes even logos and links. *This information can be a goldmine for cyber criminals.* They can manipulate these details to create convincing phishing emails, where they'll pretend to be someone you trust. This can lead to data breaches, financial loss, and a damaged reputation.

Why is this a problem?

Firstly, email signatures are a cornerstone of professional communication. They're used in almost every professional email, making them a perfect target for cyber attackers.

Secondly, the information in signatures is often static and rarely updated with security in mind, making it easier to spoof or misuse them.

The overlooked dangers include:

PHISHING ATTACKS: Cyber criminals use familiar signatures to create deceptive emails that trick recipients into revealing sensitive information.

SPOOFING: Attackers create fake email addresses and signatures to impersonate trusted contacts, leading to fraudulent activities.

MALWARE AND RANSOMWARE: Links or attachments within a spoofed signature can install harmful software on a recipient's device, compromising security and data integrity.

Despite these risks, many organisations don't prioritise the security of their email signatures. They're seen as a formality or a branding tool rather than a potential security threat. This lack of awareness can leave institutes exposed to significant risks.

Understanding the basics

LET'S KICK THINGS OFF WITH A SIMPLE QUESTION: What exactly is an email signature? At first glance, it seems like a no-brainer. It's that neat little block of text at the end of our emails that says who we are and how to get in touch with us.

However, there's a lot more to it than just a name and a phone number. Email signatures can include your company logo, job title, contact information, social media links, and sometimes even a personal sign-off or legal disclaimer.

Now, here's where it gets interesting – and a bit alarming. Most of us never think about the **security implications** of these signatures. We see them as a professional necessity, a way to make our emails look polished and trustworthy. However, for cyber criminals, email signatures can be a goldmine.

Think about it. Your email signature is a digital business card. It's in every email you send, seen by colleagues, clients, parents, students, or anyone else you communicate with. This consistency is great for branding and trust-building, but it also makes it an attractive target for those with malicious intent.

Cyber criminals can use the information in your signature to create highly convincing phishing emails. These emails look and feel legitimate because they mimic the exact format and style of your regular communications. All it takes is a little bit of your information – your name, job title, and company logo – and they're halfway to creating a scam that could trick even the most vigilant among us.

Imagine that one day, you receive an email that looks like it's from a supplier. Their email signature matches the email signature in all their other emails perfectly: Same logo, same layout, same contact information. You don't give it a second thought, but the email isn't from your supplier. It's from a cyber criminal who's managed to spoof the signature. You click the link, and just like that, you've been scammed.

This isn't just a one-off incident. It's a common tactic used in phishing attacks. When a phishing email looks as genuine as that, it's easy to see how even the savviest person could be fooled.

Breaking down

What makes email signatures so vulnerable? Here are a few key points to consider…

PERSONAL AND PROFESSIONAL INFORMATION: Your email signature often includes detailed information about you and your organisation. This data can be used to create convincing fake emails that appear to come from you.

CONSISTENCY AND FAMILIARITY: Your signature is consistent and familiar, which leads to recipients trust it. Cyber criminals exploit this trust by creating forged signatures that look almost identical to the real thing.

HYPERLINKS: Many email signatures include links to websites or social media profiles. These links can be manipulated to direct recipients to malicious sites, even if the link text looks legitimate.

There are some common misconceptions about email signature security that we need to clear up:

Email signatures are just for branding."

Sure, they help with branding, but they also carry information that can be misused if not properly secured.

Only big organisations need to worry about this."

Wrong. Small and medium-sized organisations are often more vulnerable because they might not have robust security measures in place.

Using a simple signature reduces risk."

Simplicity doesn't eliminate risk. Even a basic signature can be spoofed or used in phishing attacks.

To keep your email signature from becoming a security risk, start by creating consistency across your organisation. When everyone's signature looks the same, it's easier to spot anomalies. Verify any links included in your signature to make sure they point to secure, legitimate websites. Also remember, less is more – only include information that's necessary.

It's crucial to educate your team about the importance of email signature security. Make sure everyone knows the risks and understands how to spot suspicious emails, even if they look familiar.

Identifying common threats

Cyber threats come in many shapes and sizes and understanding them is the first step to defending against them. Let's break down some of the most common threats associated with email signatures and how they can wreak havoc on your organisation.

Phishing

Phishing is perhaps the most well-known cyber threat, and for good reason. Email signatures play a crucial role in these attacks because they add a layer of credibility.

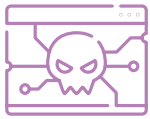
Let's say you've had an email that appears to be from your bank. The email looks legitimate, the language is formal, and at the bottom, there's a familiar signature from someone you've corresponded with before. Everything seems in order, so you click the link to update your account information. What you don't realise is that the email is fake, the link leads to a malicious website, and you've just handed over your details to a cyber criminal.

Spoofing

Spoofing is all about deception. It's when an attacker forges the email header, making it look like the email is coming from someone you trust. The email signature is a critical part of this illusion. By replicating the signature down to the smallest detail, attackers can make their emails appear authentic.

Consider a scenario where you receive an email from a colleague asking for some confidential information. The email address looks correct, and the signature is identical to the one you're used to seeing. Without a second thought, you respond with the information. Later, you discover that your colleague never sent that email. It was a spoofed message, and now your sensitive information is in the wrong hands.

Malware



Malware, short for malicious software, includes viruses, worms, and Trojans designed to cause damage or gain unauthorised access to your system. Email signatures can inadvertently be a part of malware attacks, especially when they include hyperlinks or attachments.

Picture this: You get an email from a known vendor with a contract attached. The email signature includes their logo, contact information, and a link to their website. Trusting the source, you download the attachment and open it. Uh-oh… the attachment contains malware that infects your system, compromising your data and potentially spreading throughout your network.

Ransomware

Ransomware is a type of malware that locks your data or system, demanding a ransom to unlock it. It often spreads through malicious email attachments or links. Cyber criminals can use spoofed email signatures to make their ransom demands seem more legitimate and urgent.

Imagine receiving an email from your IT department with an urgent security update. The email insists that you download the attached file immediately. The signature at the bottom looks exactly like the one your IT manager uses, so you comply. Moments later, your screen is locked, and a ransom note appears, demanding payment to regain access to your data. The email was fake, and now your organisation is at a standstill.

Data leakage

Email signatures can sometimes include more information than necessary, making them a potential source of data leakage. Cyber criminals can use the details in signatures to piece together information about your business, which can then be used for targeted attacks.

For instance, if your email signature includes your full name, job title, and department, an attacker can use this information to create a highly targeted **phishing email.** They might even call your office, posing as a colleague or client, leveraging the information gleaned from your signature to gain your trust.

Creating secure email signatures

Now we understand why email signatures can be a real target for cyber threats, how can you create a secure email signature that's not just professional but is also safe?

First things first, simplicity is your friend. Think firm, friendly, and straightforward. When it's cluttered with too much information or fancy graphics, it not only looks messy but also becomes a playground for cyber criminals to hide malicious content.

Stick to the basics: Your full name, job title, company name, and contact information. These are the essentials that people need to know. If you feel the urge to add more, remember that less is often more in terms of security. The more information you provide, the more ammo a potential attacker has. Avoid adding unnecessary graphics or using multiple fonts. Standard, widely recognised fonts are your safest bet.

Links in email signatures are incredibly useful but can also be dangerous if not handled correctly. Always verify that any links you include point to legitimate, secure websites. Hover over the link to check the actual URL – this simple step can save you from a lot of trouble. Instead of using vague anchor texts like "Click here," use full URLs. It might not look as sleek, but it provides transparency about where the link will take the recipient.

Having a standardised email signature format for your entire company is important. It not only looks professional but also helps recipients recognise genuine emails from your team. Implementing a company-wide template makes sure that everyone's on the same page and makes managing security much easier. Plus, a cohesive look strengthens your brand image.

Regular updates to your email signature are also important. Make it a habit to review and update it regularly to reflect any changes in your contact information, job title, or company details. Outdated information can be exploited, so keeping everything current minimises this risk.

Now, here's a cool tech tip: Consider using digital signatures. These are like encryption for your email, verifying that the message is from you and hasn't been tampered with. It adds an extra layer of security, assuring recipients that your email is genuine.

Once again, educating your team is equally important. Even the most secure email signature won't protect your organisation if your staff aren't aware of the potential risks. Make sure everyone knows about the dangers of phishing and spoofing, and how to spot suspicious emails. Providing clear guidelines on what information to include in their signatures and how to handle links and attachments can go a long way in preventing security breaches.

Let's not forget about regular audits and monitoring. Set up routine checks to make sure all email signatures across your organisation comply with your guidelines. Look for inconsistencies or outdated information that could be exploited. Using monitoring tools can help you keep an eye on email traffic and detect any unusual activity that might indicate a security breach. Immediate alerts can help you respond quickly and effectively to potential threats.

Implementing encryption and other security measures

Alright, you've nailed the basics of designing a secure email signature. Now, let's add some muscle with encryption and other essential security measures.

Think of encryption as a way to lock up your email content so tightly that only the intended recipient has the key to unlock it. When you send an email, encryption scrambles the content into a code that can only be deciphered by someone with the correct decryption key. Even if someone intercepts your email, they won't be able to read it.

Digital signatures are a fantastic example of this in action. They're a bit like digital fingerprints – they verify the sender's identity and confirm that the email hasn't been tampered with. When you use a digital signature, you're essentially saying, "Yes, this email really is from me, and it hasn't been altered." This adds an extra layer of trust and security to your communications.

Most modern email platforms (including Outlook) support digital signatures. You'll need a digital certificate, which you can get from a trusted Certificate Authority (CA). Once you have your certificate, it's just a matter of setting it up in your email software (we can help with this).

There are other encryption methods you can use to protect your emails too. One common approach is to encrypt the entire email message and its attachments.

This makes sure that all the content of the email is protected, not just the signature. Again, most email platforms support this feature, and it can usually be enabled with just a few clicks in your email settings.

Another powerful tool in your security arsenal is two-factor authentication (2FA). If you haven't already enabled this, now is the time. 2FA adds an extra step to your login process, usually involving a code sent to your phone or generated by an app. It makes it much harder for cyber criminals to gain access to your email account, even if they somehow get hold of your password.

Next, you have secure email gateways, the bouncers of your email system. They monitor incoming and outgoing emails for threats and block anything suspicious. Secure email gateways can filter out phishing attempts, malware, and other nasty stuff before it even reaches your inbox.

Also don't forget about regular audits and monitoring. It's not enough to set everything up and forget about it. Regularly reviewing your security settings and practices is crucial. This means checking that your encryption settings are up to date, making sure digital certificates haven't expired, and verifying that 2FA is enabled for all accounts.

Monitoring tools are also a big help here. They can keep an eye on your email traffic and alert you to any unusual activity, such as multiple failed login attempts or emails being sent from unfamiliar locations. These alerts can give you an early warning that something might be wrong, letting you act before any real damage is done.

Understanding the risks involved with your email signature is the first step to keeping them safer and more secure. Just as you don't want to fall for a spoofed email signature, you also don't want your company's email signatures to be spoofed to scam others.

We are experts in every aspect of security, including email signatures.

Get in touch.

www.breathetechnology.com
(live chat available)

London 020 3519 0124
Cambridge 01223 209920
Sheffield 0114 349 8054
Suffolk 0144 059 2163

lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms
EMPOWERING YOU THROUGH SECURE TECHNOLOGY