CUSTOMERONE

Symantec

Digital Signatures:

HOW A SIMPLE ICON HELPS THWART EMAIL FRAUD

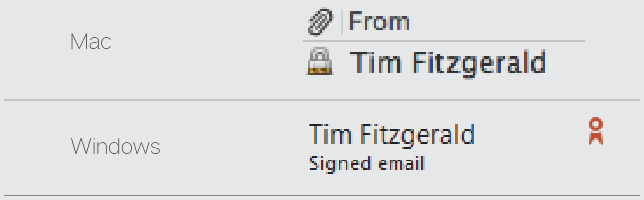
Suppose your CEO emails your finance department and asks you to wire $100,000 to an international account as part of critical but secret negotiations.

Or your CTO emails you and asks for a batch of proprietary source code. Or a VP emails you looking for confidential customer information.

Of course you want to be responsive. But you also know you need to tread carefully when it comes to distributing sensitive information, even within the company. So how do you proceed?

There's one simple first step—confirm the email is legitimate by looking for a digital signature. If the email was digitally signed it'll be tagged in your Outlook inbox with an icon: a **red ribbon in Windows**, a **lock on a Mac**.

The icon tells you the email is genuine, and not a hacker's attempt to spoof the sender's name. If you see the icon you know you can comply with the request with confidence. And if you don't see it, you know you need to confirm the request before fulfilling it.



Mac

From

Tim Fitzgerald

Windows

Tim Fitzgerald

Signed email

When someone sends you a digitally signed email, Outlook tags it with an icon: a lock on a Mac and a red ribbon in Windows.

At Symantec we've developed a wide-ranging program to help protect our employees from malicious emails. Our strategy encompasses everything from exhaustive training to Symantec products such as Email Security.cloud. This paper focuses on one aspect of our overall story: **digital signatures**.

By validating our emails with unique digital signatures, we strike a major blow against phishing attacks. This paper explains why we launched an effort in 2016 to roll them out to every Symantec employee around the world. Stay tuned for Part 2 of this story, when we look back at how the rollout went and explain the shortcuts we developed to speed up the process.

Before we get into details, let's be clear on one important point: A digital signature is **NOT** related to the email signature that you compose yourself and append to the bottom of your messages (those are easy to forge). Nor is it related to a scanned signature, in which an email sender attaches a virtual image of his or her autograph. Instead, it's a digital flag that validates an email message as authentic based on the presence of a unique identifier that can't be modified.[1]

> **Unlike the ordinary email signature that you compose yourself and append to the bottom of your messages, a digital signature is an automated 'seal of approval' that proves your email is authentic.**

Digital signatures are an easy and relatively inexpensive way to strengthen your security profile. Historically, however, we've seen that some companies have been slow to embrace them, for a few reasons:

1. The process to configure them used to be unwieldy;
2. Phishing, the threat they're designed to thwart, wasn't always as big a problem as it is today; [2]
3. People didn't know enough about them to understand the value relative to the expense.

As we'll demonstrate, there's no longer an excuse not to use them. They've become simple enough to administer that your IT folks can set them up in minutes. More important, the protection they provide is increasingly vital—a single phishing attack can cost your company six figures or more, so it behooves you to enable digital signatures for your entire company: employees, contractors, and anyone else who uses your corporate email network.

Getting started with a digital certificate

If you wrote a letter in the Middle Ages, you might have sealed the envelope with a dollop of hot wax. Then, to prove the letter was written by you, you might have pressed a distinctive seal or signet ring into the cooling wax, producing a unique impression that confirmed the message was no forgery.

Today a digital signature serves much the same purpose. Each one is unique to its user and virtually impossible to copy, so it allows a sender to affirm his or her email as authentic while also assuring the recipient that the message is genuine and wasn't modified in transit.

To be clear, a digital signature doesn't actively do anything on its own. It's an icon that merely signifies that the verification process was carried out behind the scenes, and the sender's identity has been confirmed.

That unseen process might seem a little technical. So we'll explain it with a simple analogy: In the real world, you can use your driver's license to prove that you are who you say you are. Everyone agrees to trust your license because we trust that the DMV vetted you before granting the license. Likewise, to prove your identity in the online world, a similar trusted agency called a certificate authority (CA) will vet you, confirm who you are, and issue a form of ID that we all agree to trust. That online ID is called a **digital certificate**.

The certificate authority will verify that your email has been configured so the name on the "From" line of your email matches your name exactly—down to the capitalization of individual letters. (Some digital certificates verify your organization as well.) Then the CA issues you a digital certificate, which you download and install on a single specific device.

Next you'll configure your Outlook settings on that device such that every email you send from it will have both your digital signature and the icon of a ribbon or lock. Recipients will be able to click on the icon to see which CA issued your certificate and when it's set to expire.

(If you try to change how your name appears after you've installed the digital certificate, the recipient will see a banner cautioning that the name on the email doesn't match the name on the certificate.)

"What if my laptop is stolen and the thief sends an email with my digital signature? How is the recipient supposed to know it's fraudulent?"

This is one of the most common questions we get. This scenario is possible, but the thief would need more than your computer—he'd also have to have the usernames and passwords for your computer and email account. If he does have that level of information on you, your security is already so far compromised that he can do far worse to your corporate network than send a simple phishing email.

"Once a hacker has your username and password, they don't need to impersonate you, they *are* you, for all intents and purposes," says Craig Morea, Symantec senior manager of information security.

(Consider this yet another reminder to **always** protect your hardware and software with strong passwords).

Making digital signatures a Symantec-wide priority

For Symantec employees, acquiring a digital signature takes about five minutes. First the user requests a digital certificate from our authentication team. Then, after the team approves the request, the user is sent a link from which to download his or her unique digital certificate.

[We can serve as our own CA because we acquired VeriSign, one of the world's best-known certificate authorities. To obtain your own digital certificates from Symantec, start here: https://www.symantec.com/products/information-protection/digital-ids-secure-email]

Even though our setup process is simple, we didn't always mandate that every employee have a digital signature. That's because there wasn't an obvious business need for all 11,000 Symantec employees and contractors. We did require them of specific staffers, such as our legal team and those at or above the director level, but it was only after we started seeing an increase in phishing attempts that we knew we needed to step up our protection. So in 2016 we made digital signatures a companywide priority.

Other companies and agencies have adopted similar strategies. For example, the U.S. Department of Defense requires employees to digitally sign any email that contains an attachment or link.[3]

So should your company mandate digital signatures as well? At CustomerONE we recommend that you do—they're a simple, low-cost way to neutralize some of the most common and effective phishing schemes.

At a minimum we advise that your executives have them. After all, they're the people who phishers are likely to impersonate. You'll also need to train your employees to look for digital signatures and know how to interpret them.

What it means to get an email that is or isn't digitally signed

If you're like us, once you start using digital signatures you'll find yourself automatically noticing whether incoming emails have been digitally signed.

"Everyone on my team has a digital certificate. So when an email comes in without one, it sticks out like a sore thumb," says Craig Morea, our senior manager of information security. "So we'll stop and look at it and ask why it's different."

If the email is just from a co-worker inviting him to lunch he won't stress about it. But if it requests something important or confidential, such as financial data, he won't reply right away. Instead he'll either call the sender for confirmation or refer the email to our IT security desk for further investigation.

Often there turns out to be a simple explanation—and it usually has to do with smartphones. Recall that for the most part a digital certificate can only be installed on a single device. So if you install yours on your laptop, only the emails you send from that machine will have a digital signature. If you decide you want to send digitally signed emails from your smartphone or other device as well you'll have to take the extra step of exporting the digital certificate to those devices too.

There's one other common issue with smartphones. For some popular phones, the option to enable digital signatures (the option shows up as S/MIME) is grayed out as a default. As long as the option is disabled, you can neither send digitally signed emails nor tell if an incoming email has a digital signature—the telltale ribbon or lock icon will be absent. The solution involves a simple IT fix so it's not a big deal—it's just one more setting that has to be set up just right.

At this point you might be thinking that the whole setup process seems painstaking. It absolutely is—because it has to be. This is technology designed to thwart impersonators, so every last setting has to be fine-turned down to the most meticulous detail.

But don't let that dissuade you. We recommend that customers leave the setup process to their IT staffers. They'll know which settings to adjust, which features to enable/disable, etc. It's not that complicated, but people who know exactly what they're doing can have you set up in minutes. And once you're set up, you won't see a difference—you'll send and receive emails exactly as before. The only change you'll notice is the shiny new icon on your emails—an icon that tells you you've taken a simple but significant step toward making your company more secure.

Contact us for more information

This paper was meant to give you a brief overview of digital signatures. If you'd like more details or clarification we invite you to visit our website, where you can contact a Symantec representative who'll be happy to serve you:
https://www.symantec.com/products/information-protection/digital-ids-secure-email

We also invite you to learn more about Symantec's other products and services. Our CustomerONE series of nontechnical stories is available here:
https://www.symantec.com/about/customerone

› CONTACT SYMANTEC TODAY

[1] You'll often see the topic of digital signatures discussed in conjunction with encryption efforts. For simplicity we'll leave encryption for a separate story.

[2] For more information on how Symantec fights back against phishing attacks see: Phish Fight: Empowering Our Employees Against Con Artists

[3] http://www.navy.mil/submit/display.asp?story_id=42771

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

Symantec's CustomerONE team can facilitate discussions between you and our IT security practitioners to help you address your security questions and concerns. Please contact us directly or through your Symantec sales team.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.