THE CONVERSATION
Academic rigor, journalistic flair

The only safe email is text-only email

September 10, 2017 8.40pm EDT

Authors

Sergey Bratus
Research Associate Professor of Computer Science, Dartmouth College

Anna Shubina
Post-doctoral Associate in Computer Science, Dartmouth College

For safety, look to text-only messaging. The Conversation, via picascii.com, publicdomainpictures.net and kelvinsong, CC BY-ND

It's troubling to think that at any moment you might open an email that looks like it comes from your employer, a relative or your bank, only to fall for a phishing scam. Any one of the endless stream of innocent-looking emails you receive throughout the day could be trying to con you into handing over your login credentials and give criminals control of your confidential data or your identity.

Most people tend to think that it's users' fault when they fall for phishing scams: Someone just clicked on the wrong thing. To fix it, then, users should just stop clicking on the wrong thing. But as security experts who study malware techniques, we believe that thinking chases the wrong problem.

The real issue is that today's web-based email systems are electronic minefields filled with demands and enticements to click and engage in an increasingly responsive and interactive online experience. It's not just Gmail, Yahoo mail and similar services: Desktop-computer-based email programs like Outlook display messages in the same unsafe way.

Simply put, safe email is plain-text email – showing only the plain words of the message exactly as they arrived, without embedded links or images. Webmail is convenient for advertisers (and lets you write good-looking emails with images and nice fonts), but carries with it unnecessary – and serious – danger, because a webpage (or an email) can easily show one thing but do another.

Returning email to its origins in plain text may seem radical, but it provides radically better security. Even the federal government's top cybersecurity experts have come to the startling, but important, conclusion that any person, organization or government serious about web security should return to plain-text email:

> *"Organizations should ensure that they have disabled HTML from being used in emails, as well as disabling links. Everything should be forced to plain text. This will reduce the likelihood of potentially dangerous scripts or links being sent in the body of the email, and also will reduce the likelihood of a user just clicking something without thinking about it. With plain text, the user would have to go through the process of either typing in the link or copying and pasting. This additional step will allow the user an extra opportunity for thought and analysis before clicking on the link."*

Misunderstanding the problem

In recent years, webmail users have been sternly instructed to pay perfect attention to every

nuance of every email message. They pledge not to open emails from people they don't know. They say they won't open attachments without careful vetting first. Organizations pay security companies to test if their employees make good on these pledges. But phishing continues – and is becoming more common.

News coverage can make the issue even more confusing. The New York Times called the Democratic National Committee's email security breach somehow both "brazen" and "stealthy," and pointed fingers at any number of possible problems – old network security equipment, sophisticated attackers, indifferent investigators and inattentive support staff – before revealing the weakness was really a busy user who acted "without thinking much."

But the real problem with webmail – the multi-million-dollar security mistake – was the idea that if emails could be sent or received through a website, they could be more than just text, even webpages themselves, displayed by a web browser program. This mistake created the criminal phishing industry.

Engineered for danger

A web browser is the perfect tool for insecurity. Browsers are designed to seamlessly mash together content from multiple sources – text from one server, ads from another, images and video from a third, user-tracking "like" buttons from a fourth, and so on. A modern webpage is a patchwork of third-party sites, which can number in the dozens. To make this assemblage of images, links and buttons appear unified and integrated, the browser doesn't show you where the pieces of a webpage come from – or where they'll lead if clicked.

Worse, it allows webpages – and thereby emails – to lie about it. When you type "google.com" into your browser, you can be reasonably sure you will get Google's page. But when you click a link or button labeled "Google," are you actually heading to Google? Unless you carefully read the underlying HTML source of the email, there are a dozen ways your browser can be manipulated to trick you.

This is the opposite of security. Users can't predict the consequences of their actions, nor decide in advance if the potential results are acceptable. A perfectly safe link might be displayed right next to a malicious one, with no apparent difference between them. When a user is faced with a webpage and the decision to click on something, there is no reasonable way to know what might happen, or what company or other party the user will interact with as a result. By design, the browser hides this information. But at least, when browsing the web, you can choose to start at a trusted site; webmail, however, delivers an attacker-made webpage right into your mailbox!

The only way to be sure of security in today's webmail environment is to learn the skills of a professional web developer. Only then will the layers of HTML, Javascript, and other code become clear; only then will the consequences of a click become known in advance. Of course, this is an unreasonable level of sophistication to require for users to protect themselves.

Until software designers and developers fix browser software and webmail systems, and let users make informed decisions about where their clicks would lead them, we should follow the advice of C.A.R. Hoare, one of the early pioneers of computer security: "The price of reliability is the pursuit of the utmost simplicity."

Safe email is plain-text email

Companies and other organizations are even more vulnerable than individuals. One person needs only to worry about his or her own clicking, but each worker in an organization is a separate point of weakness. It's a matter of simple math: If every worker has that same 1 percent chance of falling for a phishing scam, the combined risk to the company as a whole is much higher. In fact, companies with 70 or more employees have a greater than 50 percent chance that someone will be hoodwinked. Companies should look very critically at webmail providers who offer them worse security odds than they'd get from a coin toss.

As technologists, we have long since come to terms with the fact that some technology is just a bad idea, even if it looks exciting. Society needs to do the same. Security-conscious users must demand that their email providers offer a plain-text option. Unfortunately, such options

are few and far between, but they are a key to stemming the webmail insecurity epidemic.

Mail providers that refuse to do so should be avoided, just like back alleys that are bad places to conduct business. Those online back alleys may look eye-pleasing, with ads, images and animations, but they are not safe.

This article was written in collaboration with cybersecurity researcher and developer Robert Graham.

Web browsers Email Cybersecurity Yahoo Gmail Phishing Spearphishing