UNDERSTANDING PHISHING

INKY

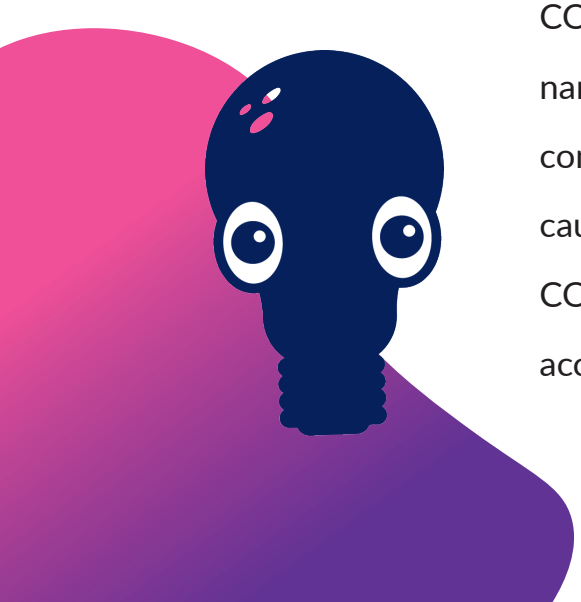
Exploiting a Pandemic

White House COVID-19 Phishing Scams

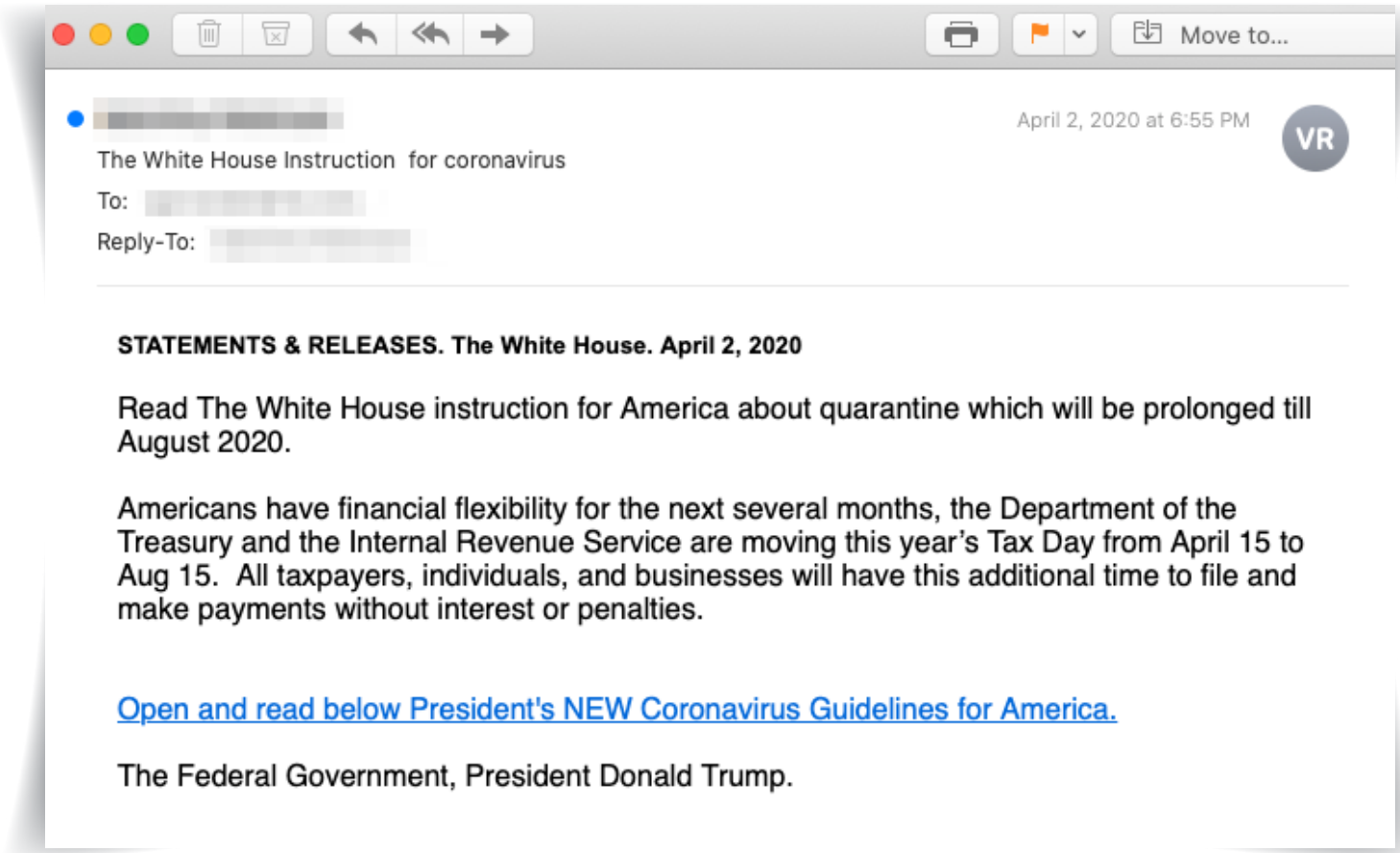
We are facing unprecedented times, and we may be on the cusp of one of the biggest phishing waves in history. COVID-19 phishing attacks are now impersonating the White House and President Trump. Take a look at some of the most recent scams we've caught.

Skyrocketing COVID-19 Phishing attacks are now impersonating the White House and President Trump. It's enough that we are dealing with a global pandemic, a time when all nations should be joining in support of each other to get through this crisis. It's unfortunate that these evil criminals are using phishing attacks to prey on workers at home, when our guard is down, to entice us to click on their malicious links. We are facing unprecedented times, and we may be on the cusp of one of the biggest phishing waves in history.

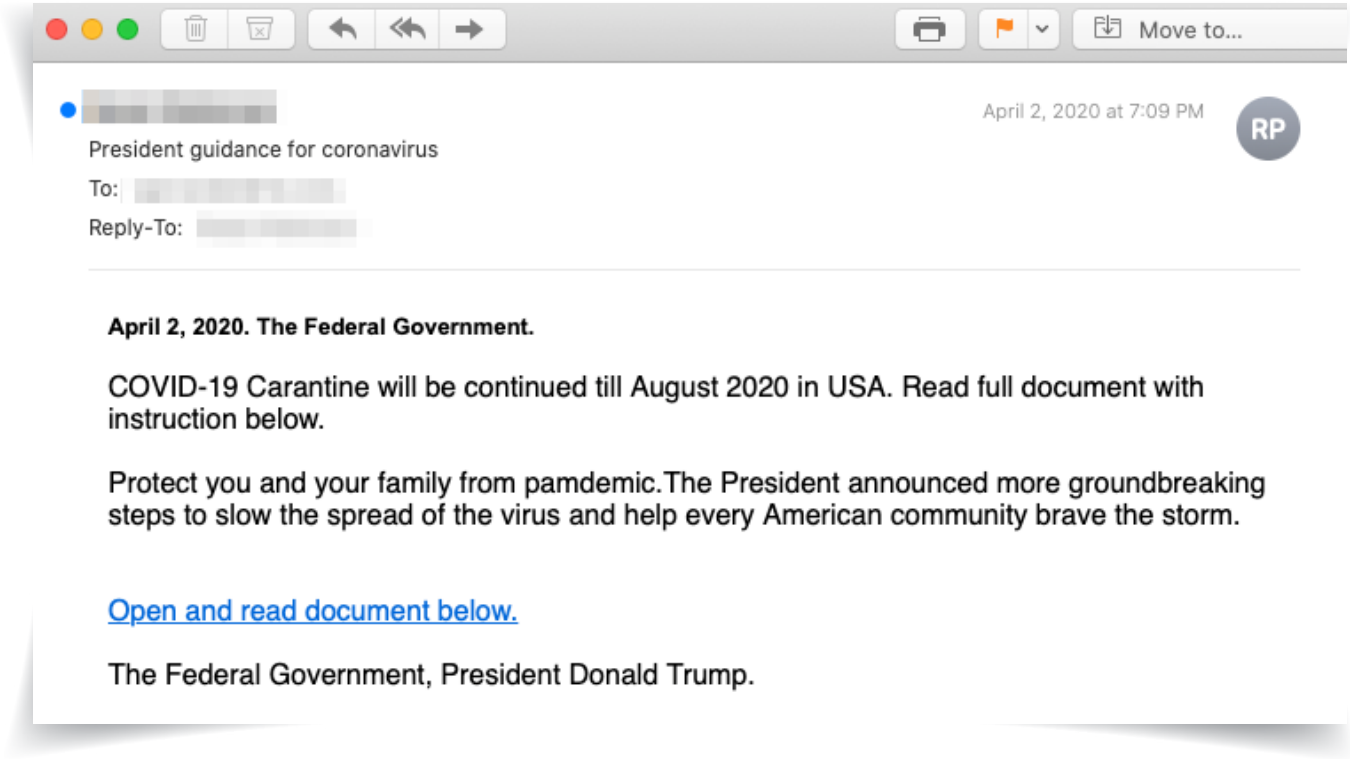
In an earlier installment of *Understanding Phishing* we examined some COVID-19 themed phish that INKY has caught in the wild. We continue to see an uptick in phishing emails throughout this crisis, and we've seen new types of phishing attempt we're calling 'Coronaphish'. Most of these phish are driven from templates the attackers compile using a list of victim companies and emails. It's similar to Mad Libs: the criminal's template has most of the (fixed) text, and his script fills in the blanks (variables) to better target the phish to the recipient. A victim might receive an otherwise-generic COVID-19 email that has her company and CEO's name inserted into the right place so it looks really convincing... It's a bit like evil mail merge. Recently we caught a couple remarkably credible but purely static COVID-19 phish. The attacker(s) sent both from mail accounts hosted in Russia. Let's take look.



First we have a mail titled *The White House Instruction for coronavirus*, supposedly from a Valentina Robinson. Here's a screenshot:



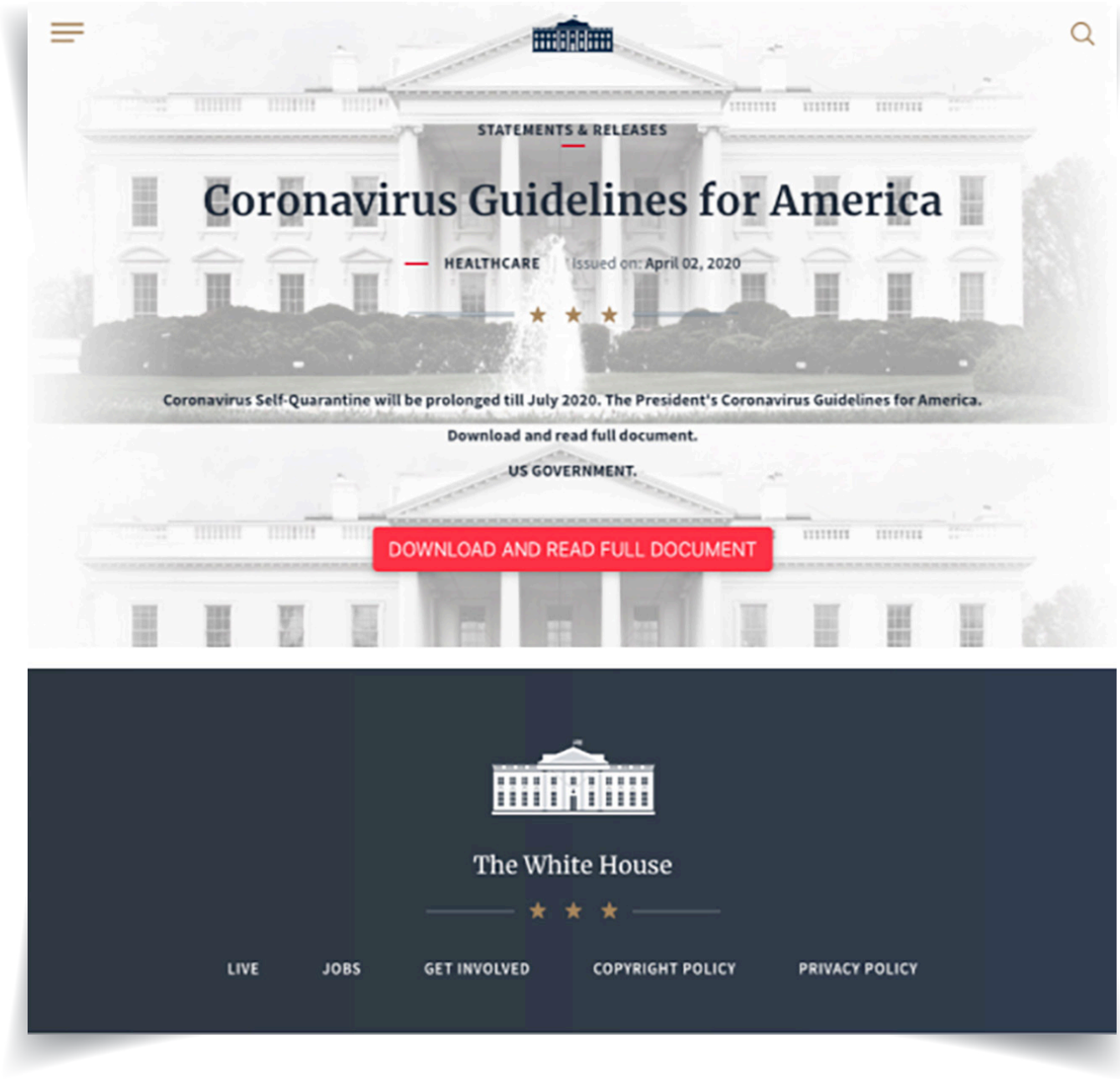
The second is quite similar, but comes from a different email address from the same mail domain and a different sender name:



Aside from impersonating President Donald Trump — we are to believe, evidently, that Valentina and Rosie are presidential spokesphishers — both seem to predict the quarantine will last until August 2020. The first correctly states the tax filing deadline has been delayed, but gets the date wrong: instead of August 15, 2020, the date has actually been changed to July 15, 2020.

Neither missive seems quite up to either the grammatical or typographical standards of the White House: in the second email we're instructed to "Read full document," and both quarantine and pandemic are misspelled.

Nevertheless, it's easy to imagine a few overloaded working-from-home employees falling for these. So what happens when they click through? Well the site has been taken down now, but when these emails first arrived click-through took us here:



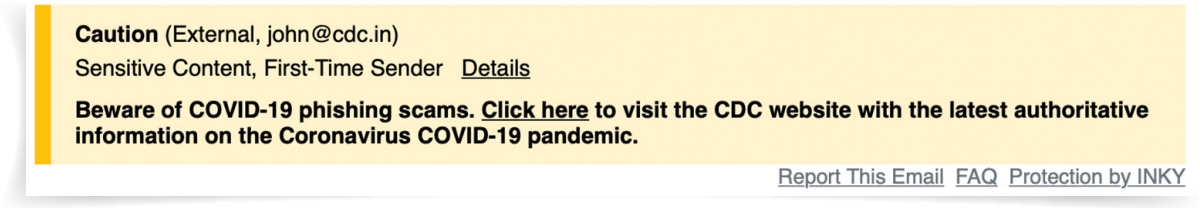
Looks pretty good, right? That's because it's an exact HTML and CSS replica of the exact content on the real White House Coronavirus informational site at the time these emails arrived.

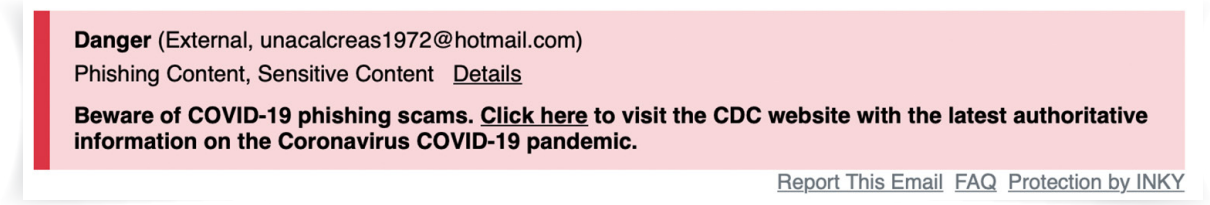
This raises a point we often make at INKY: the attacker's easiest path to creating convincing fakes is *not to create any content at all*, but simply to copy a real email or website.

The only difference between the attacker's replica site and the real White House site is what happens when the user clicks on the button labeled *Download and Read Full Document* — in the case of the attacker's button, the Microsoft Word document the user is given contains macros that install malware!

INKY®

At INKY we work hard to stay abreast of phishing scams as they evolve over time, and we continue to develop general countermeasures against the increasingly sophisticated tactics attackers use. INKY has developed unique COVID-19 banners to provide an extra layer of awareness — perfect for newly remote employees who may be distracted by elements of their new work environment.





We're passionate about email.

Want to talk about an issue you're facing in email security at your organization?

Request a demo today

www.inky.com