KnowBe4
Human error. Conquered.

Security Awareness Training Blog

24 Aug

A State-of-the-Art Spoof (or, Why Turning Your Users Into Grammar Nazis Won't Keep the Bad Guys Out)

Stu Sjouwerman

By Eric Howes, KnowBe4 Principal Lab Researcher. Malicious actors are becoming very skilled at exploiting popular online services that enjoy the familiarity and trust of millions of users. And the phishing emails landing in users' inboxes are, likewise, becoming ever more dangerous and difficult to detect.

In some cases the bad guys use compromised accounts at popular online services to host and distribute their malicious files. Here's a short list of well-known services/brands we've seen exploited in this fashion.

- Microsoft OneDrive/Sharepoint
- Google Docs
- Dropbox
- WeTransfer
- Constant Contact (rs6.net)
- Evernote

We could add to the above list at least a half-dozen other, smaller file-sharing services. (Note that we make no claims that the above is a complete list -- just a list of those services we happen to see commonly exploited in phishing emails reported to us by customers using the Phish Alert Button, or PAB.)

Some of these services are especially useful to the bad guys because they provide email delivery functionality, allowing malicious actors to put malicious emails distributed by the services themselves directly into users' inboxes. Emails from Dropbox and WeTransfer, for example, typically sail right through firewalls, Exchange security services, and endpoint anti-virus applications because they emanate from trusted services. Moreover, users tend to recognize and trust emails from these services.

Other online services are being exploited because they allow malicious actors to mask the true destinations of malicious URLs behind a cloak of respectability. Two such services whose URLs we've often seen being used in phishing emails recently for just that purpose are:

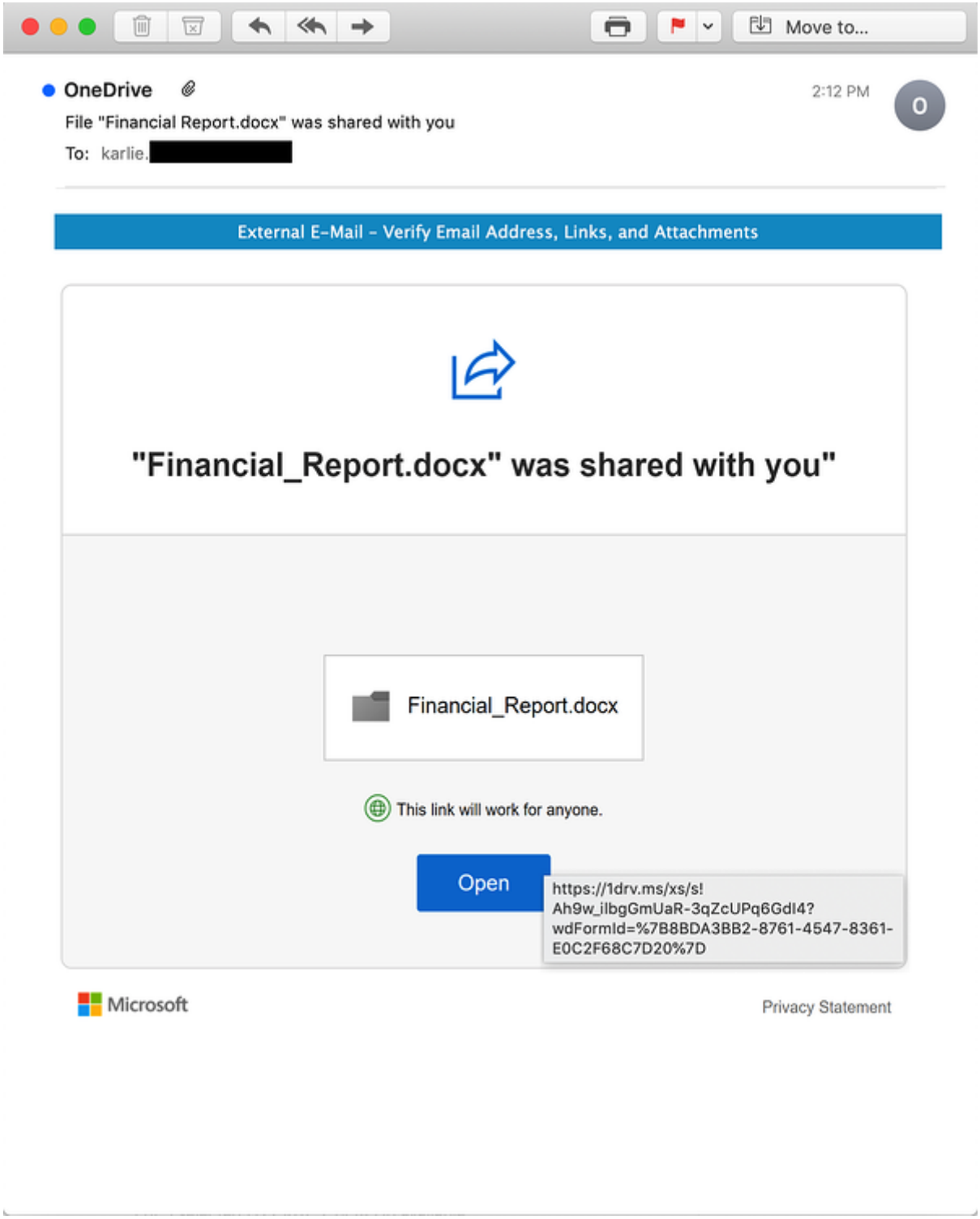
- Sendgrid (sendgrid.net)
- Hubspot (hubspotemail.net)

As before, we could supplement the above with a longer list of URL shorteners -- again, many of them familiar to users because of their widespread use in mobile applications.

And then there are the services that simply allow malicious links to be disguised in URL address bars behind fairly primitive URL redirects. Well-known domains we've seen being used recently for malicious redirection include:

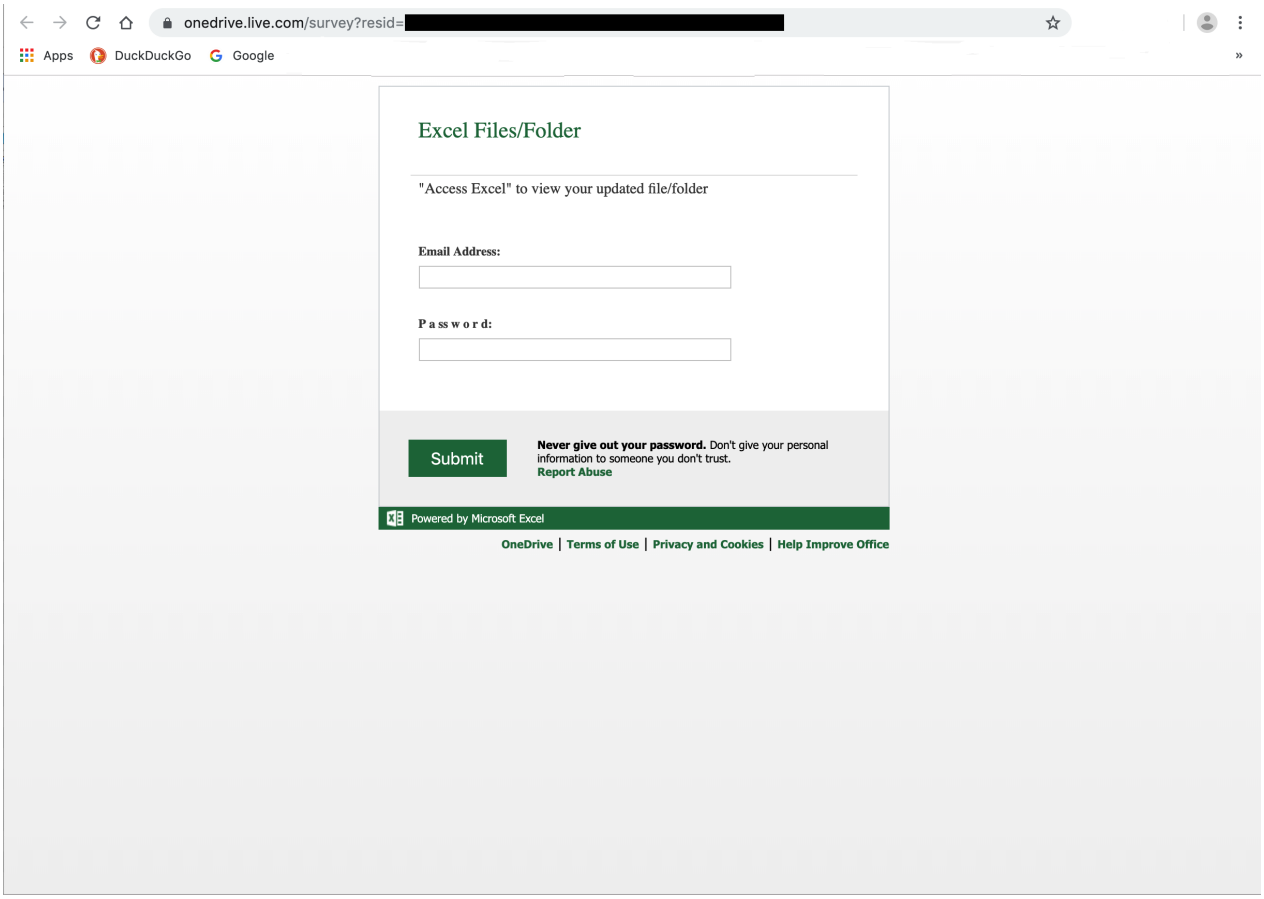
- Disqus (disq.us)
- The U.S. Social Security Administration (ssa.gov)
- Google (google.com)

Sometimes, though, exploiting these sites and services requires a bit of finesse on the part of the bad guys. Take, for example, a truly dangerous phishing email we spotted in the past few days that spoofs Microsoft OneDrive:



Although this email is indeed a spoof and not a real email from Microsoft, it is nonetheless slick, professional, and could be easily mistaken for an actual email from Microsoft. But that's not what makes it truly dangerous. Notice the link, which uses Microsoft's OneDrive URL shortener - something many users will have seen before in emails from Microsoft itself.

Clicking that link takes users to a landing page on OneDrive itself, which turns out to be a credentials phish:



In this case the bad guys smartly elected to offer up a (spoofed) Microsoft login page -- something that, again, most users would not be surprised to encounter after clicking a link to a page hosted at Microsoft itself.

In short, the branding experience in this phish is consistent from start to finish. Although the initial phishing email itself is spoofed, the malicious content is actually hosted on OneDrive. And while there are niggling little aspects of this phish that hyper-alert and religiously suspicious users might seize on to spot the ruse, we expect that most users would fail to notice anything amiss.

Even the warning about an "External E-mail" inserted by the receiving mail server at the top of the email body—something else we've seen more and more of in recent months—is of little help to users in this case. Let's break that notice down:

- *External E-mail* - well, yes, it is external, but one would expect such a notice for emails from Microsoft
- *Verify Email Address* - this might be useful if your users are in the habit of digging into email headers to verify the SPF or DKIM authentication results, but we doubt most users would bother -- even if they knew how (they don't)
- *Verify Links* - the link in this email points to a trusted online service (Microsoft OneDrive)
- *Verify Attachments* - aside from an image or two, there are no attachments to this email (the malicious content is delivered in the link)

This well-designed, state-of-the-art phish is a perfect example why the widely repeated, (hoary?) old advice to users that they learn to spot phishing emails by looking for spelling, grammar, and

syntax errors simply doesn't cut it anymore. Nor does doing annual training in the break room with a Powerpoint deck and a box of doughnuts.

The bad guys are playing for keeps, and they've learned how to exploit some of the most trusted brands on the internet in order to trick your users into coughing up the goods -- login credentials, wire transfers, W2 forms, Bitcoin ransoms, gift cards, and inside access to your network via sophisticated backdoor trojans.

When your AV endpoint fails and your employees become your last line of defense, those users need New-school Security Awareness Training to keep up. Anything short of that is an organizational disaster waiting to happen.

2019 Phishing By Industry Benchmarking Report

The 2019 Phishing By Industry Benchmarking Report compiles results from the second annual study by KnowBe4 and reveals at-risk users across 19 industries that are susceptible to phishing or social engineering attacks. Taking it a step further, the research reveals radical drops in careless clicking after 90 days and 12 months of simulated phishing testing and security awareness training.

Download Report

« Return To KnowBe4 Security Blog

Topics: Phishing, Security Awareness Training