COMODO

PHISHING GOT DARKER. AND SMARTER.

January 2018

COMODO THREAT INTELLIGENCE LAB

By Fatih Orhan
VP of Threat Labs

comodo.com/lab

Executive Summary

The Dark Art of Phishing

Phishing will remain the primary targeting method of advanced targeted attacks through 2020. This can be explained with a simple statistic:

50% **One in two users click on links in emails from unknown senders.**[1]

People are curious about the photo or website on the end of the link and often simply click on it to satisfy the urge. After an attack, they will justify their actions with statements like “But it looked exactly like an email from Apple, or Walmart, or Amazon.” or “How did they know who I receive email from?”

This Special Report studies the recent transformation in the pace and quality of phishing attacks along with recommendations for defending against them.

Millions of Phishing Attacks in 2018

Millions of business and consumer users are targets of phishing attacks every day — and many of them fall victim. Most users are not cybersecurity experts and easily take the bait of phishing traps. But where does the “black magic” of phishing hide?

Phishing is a strategy to deceive you. The goal is commonly to get you to download malware or go to a malicious website by impersonating a valid email communication and creating a feeling of urgency, either for an opportunity or a sudden loss.

[1] https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders.

Cybercriminals want to make you harm yourself using your own hands. They seek your confidential data such as personal information, usernames, passwords, credit card numbers, bank account details, etc. Getting you to volunteer such information is the easiest way to get this data. In order to manipulate you remotely, they use an explosive mix of social engineering and computer technologies to deceive you.

Faces of Phishing

A closer look at the many different types of phishing attacks.

Clone Phishing: A specific variation of phishing that intercepts a legitimate previously-delivered email and creates a malicious clone to deceive the target. The clone may differ for only one letter, a link, or a symbol. The victim easily takes it for a resend of the original email and trusts any attachments or links within.

Covert Redirect: A subtle method that relies on the original real website using open standards like OAuth 2.0 and Open ID. The attacker redirects the official open standard login towards the attacker's website. The link, URL, and website will all look legitimate because they are. The login popup will be malicious. The attack may even log the user into the legitimate website in order to keep the victim unaware that their credentials were stolen.

Filter Evasion: As organizations and vendors built filters to block phishing emails, cybercriminals used alternative content to evade them — using images instead of text so filters could not read the message. In response, cybersecurity software vendors created more sophisticated anti-phishing filters that could find hidden text in images.

Phishing: A basic phishing attack targets mass users. Cybercriminals create a malicious e-mail with a fake link. The email will look like it comes from a friend or a trusted large company like Apple or Walmart. They widely disseminate the email and wait for someone to take the bait. Phishing is wide-ranging and does not care about who the victims are.

Spear-Phishing: A more focused attack, spear-phishing seeks out specific individuals or companies (e.g. a celebrity to get credentials to their photo album or the aides to political figures). Before launching this attack, the offender gathers personal information regarding the target's friends, coworkers, or business partners. The phishing email is then tuned to the specialties of the targeted "mark." While requiring more effort, this technique is gaining in popularity due to the higher stakes involved.

Whaling: An attack stalking a "big fish" (e.g. the CEO of a credit rating company). Someone who can bring the big prize if successfully reeled in and hacked. Actually, *whaling* is the top-level of spear-phishing.

Website Forgery: Often the second component of a phishing attack. The phishing email will lure the user into visiting a forged website. Cybercriminals make it even more difficult to recognize the fake site by altering the user's address bar (e.g. use JavaScript to replace the real address bar with a picture of the bar with a with a legitimate URL).

Figure 1: An Introduction to Phishing Terms

You can buy phishing attacks online. Phishing attacks are easily created and spread rapidly. Part of the acceleration comes from these attacks now being sold as-a-service (aaS). The attacks are profitable to organized crime leading to an online "Malware Depot" with departments selling varieties of each element of a modern phishing campaign.

Anatomy of an Imaginary Phishing Attack

Meet Joanne Blackhat — an imaginary malicious hacker who wants to create a phishing attack against a company named "Big Whale" to steal secret data. What will she do?

Because she has a specific target, this will be a spear-phishing or whaling attack and Joanne needs information. At a minimum, she will need e-mail addresses for the company employees where she'll send her phishing letters. But for these letters to be effective she needs to get as much information as possible — more is always better.

Joanne will start at the Big Whale website. She extracts a lot of information about the company: who are the C-level executives; who owns the company; who are the employees; where are the employees; what are their job titles; what is the email structure used in the company; and what recent press releases were published. She will use this information to create plausible phishing e-mails. Also, Joanne can dig out even hidden information from the Big Whale website using Google dorks — special commands that help to extract data from a site. After this preliminary research, Joanne breaks out the big guns — specific software like "The Harvester" or "Maltego."

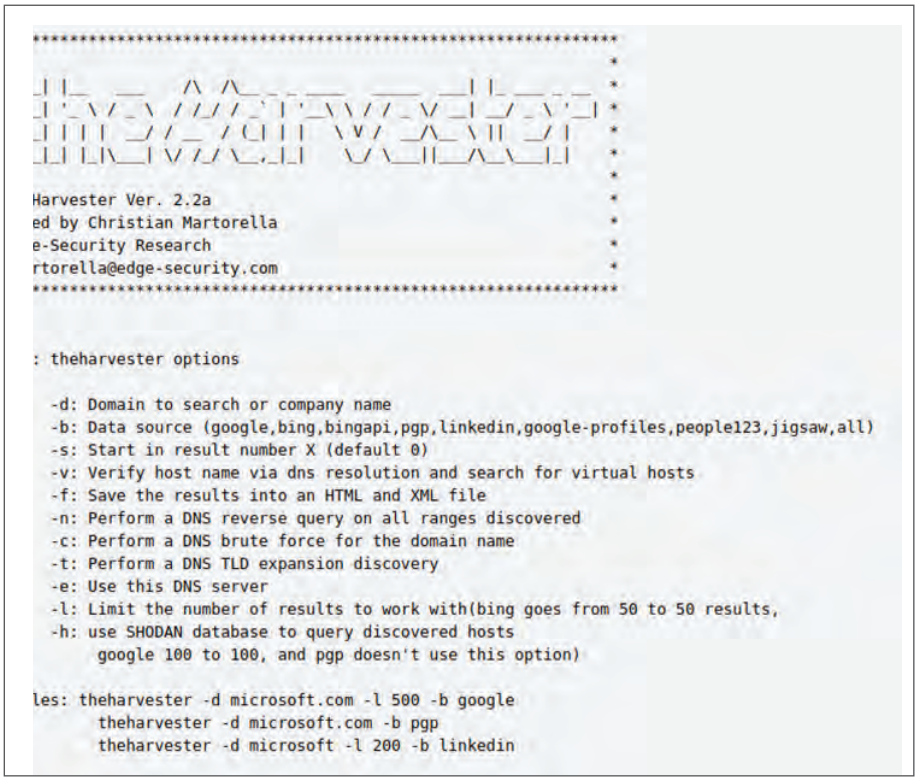

Figure 2: Screenshot of The Harvester

The Harvester scans public sources such as search engines, PGP key servers, and the SHODAN database to quickly gather target details: emails, subdomains, hosts, employee names, open ports, and banners.

Then she can will use Maltego to uncover the mail servers of the target company and messaging details such as linked email addresses. This intricate detail enables her to more easily trick her victim.

With the research phase accomplished, Joanne will now register a domain name similar to some popular website. In *Figure 3: Websites Trying to Camouflage as Comodo.com*, there are examples of sites trying to imitate www.comodo.com — the official website of cybersecurity leader Comodo. She may use a domain name close to Big Whale, or more commonly, something close to popular sites like Google, PayPal, Amazon, or WeChat.

```
tevfikd@ubuntu:~/dnstwist$ python dnstwist.py comodo.com
                                                    (1.04b)

Processing 252 domain variants .....................20%.....50%...72%.....94%. 68 hits (26%)

Original*       comodo.com      91.199.212.176 2a02:1788:2fd::b0 NS:ns0.comododns.com MX:sgmail.comodogroup.com
Addition        comodoa.com     -
Addition        comodob.com     -
Addition        comodoc.com     NS:dns16.ovh.net
Addition        comodod.com     -
Addition        comodoe.com     -
Addition        comodof.com     -
Addition        comodog.com     NS:ns1.labcc.ch MX:mail.comodog.com
Addition        comodoh.com     -
Addition        comodoi.com     -
Addition        comodoj.com     -
Addition        comodok.com     -
Addition        comodol.com     -
Addition        comodom.com     217.160.0.127 2001:8d8:100f:f000::2e2 NS:ns-es.1and1-dns.biz MX:mx00.1and1.es
Addition        comodon.com     68.178.213.61 NS:ns1.namefind.com
Addition        comodoo.com     52.71.185.125 NS:ns1.namebrightdns.com
Addition        comodop.com     -
Addition        comodoq.com     -
Addition        comodor.com     176.74.176.187 NS:ns1.uniregistrymarket.link
Addition        comodos.com     141.8.226.22 NS:ns1.gonamehost.com
Addition        comodot.com     -
Addition        comodou.com     -
Addition        comodov.com     -
Addition        comodow.com     121.9.226.10 NS:dns.bizcn.com MX:mxcom.263xmail.com
Addition        comodox.com     198.105.221.52 NS:ns1.asia.eleven2.com MX:comodox.com
Addition        comodoy.com     176.74.176.187 NS:ns1.uniregistrymarket.link
Addition        comodoz.com     157.7.188.184 NS:dns01.muumuu-domain.com MX:mail16.heteml.jp
Bitsquatting    bomodo.com      NS:ns1.uniregistry-dns.com MX:alt1.aspmx.l.google.com
Bitsquatting    aomodo.com      173.239.23.228 NS:ns1.domain-is-4-sale-at-domainmarket.com
Bitsquatting    gomodo.com      NS:ns3.dns26.com
Bitsquatting    komodo.com      216.194.173.245 NS:ns73.worldnic.com MX:inbound.komodo.com.netsolmail.net
Bitsquatting    somodo.com      202.172.25.19 NS:ns1.value-domain.com MX:somodo.com
Bitsquatting    cnmodo.com      -
Bitsquatting    cmmodo.com      -
Bitsquatting    ckmodo.com      -
Bitsquatting    cgmodo.com      -
Bitsquatting    colodo.com      35.182.144.96 NS:ns1.power-dns.com MX:mx1.ewebdevelopment.com
Bitsquatting    cooodo.com      NS:ns1.cnolnic.com
Bitsquatting    coiodo.com      -
Bitsquatting    coeodo.com      -
Bitsquatting    co-odo.com      -
Bitsquatting    comndo.com      173.239.5.6 NS:ns1.expiereddnsmanager.com MX:mx7.comndo.com
Bitsquatting    commdo.com      -
Bitsquatting    comkdo.com      NS:dns19.ovh.net MX:mx1.mail.ovh.net
Bitsquatting    comgdo.com      -
Bitsquatting    comoeo.com      -
```

Figure 3: Websites Trying to Camouflage as Comodo.com

After that, Joanne creates a copy of the site she wants to use as bait. This is as simple as a few clicks with the appropriate software. For example, Joanne can turn to a favorite of penetration testers: the Social-Engineer Toolkit or the lesser-known HTTrack website copier. Now, Joanne could just copy the original web page to her own server — but she will not.

Our imaginary Joanne is a top-level hacker, so she will find an unprotected server on the internet, break into it, and place her phishing sites there. Should the attack be discovered, this misdirection will guide police to the hapless owner of the unprotected server and Joanne effectively covered her tracks in cyberspace.

Finally, it is time for Joanne to launch her attack. She prepares her phishing email using her research to add some socially-engineered text and attaches the link to her fake site. Now she waits.

The victims do all the work by clicking on the link and giving away their credentials. Joanne now has the credentials, but she does not stop here either.

Figure 4: Result of Clicking Attachment without Auto-containment of Unknown Files

The final component of her phishing attack installs ransomware on the victim's machine. The victim gets a message as in *Figure 2: Result of Clicking Attachment without Auto-containment of Unknown Files* and now needs to decide whether paying the ransom will work to get the data back from a cybercriminal like Joanne.

A Real Site Wanting to Steal Your Information

The Comodo Threat Intelligence Laboratory blacklisted the domain name www.bestcoffeedrinks.com. Why? Look at *Figure 5: bestcoffeedrinks.com Displays a DocuSign and Google Gmail Authentication Page,* it displays both a DocuSign and Google Gmail authentication page; and you see something strange — a coffee-related site wants you to login to DocuSign. It does not stop there.

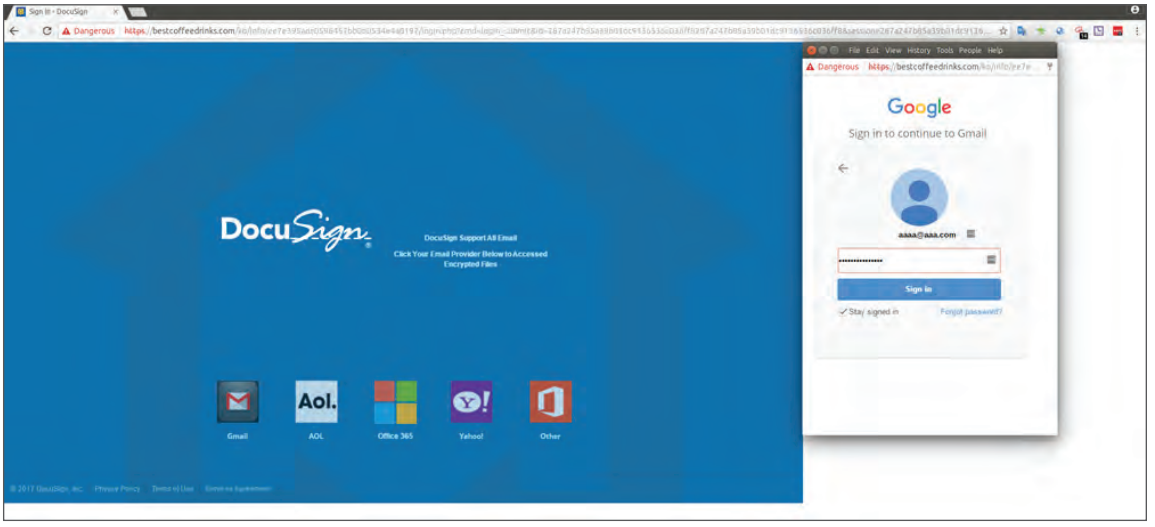

Figure 5: bestcoffeedrinks.com Displays a DocuSign and Google Gmail Authentication Page

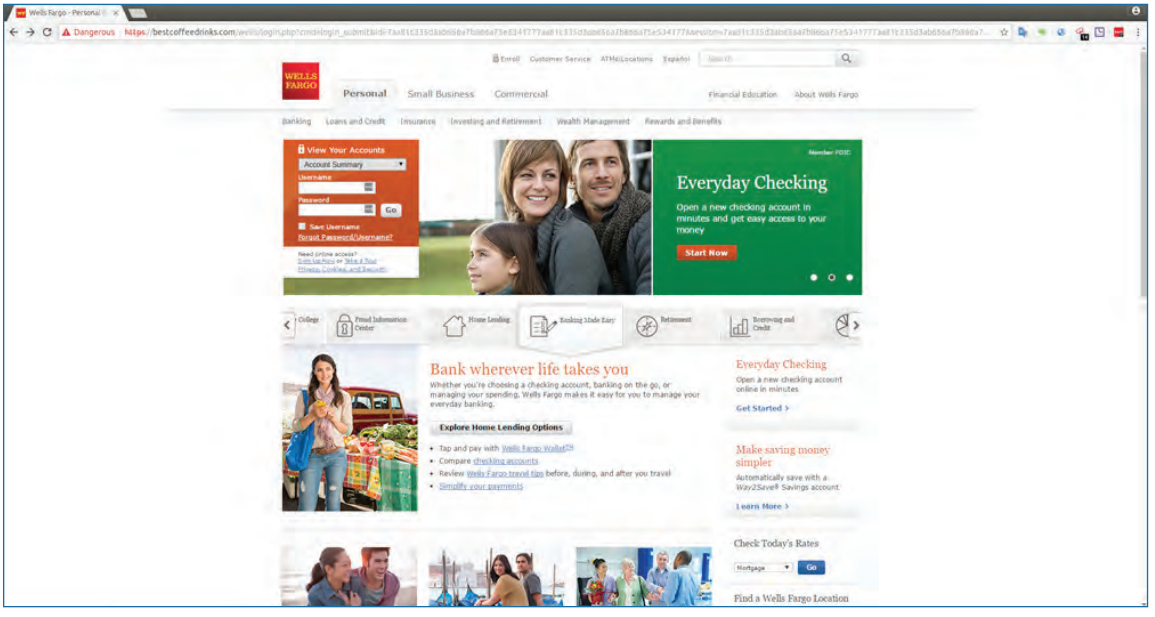

Figure 6: bestcoffeedrinks.com Displays a Wells Fargo Authentication Page

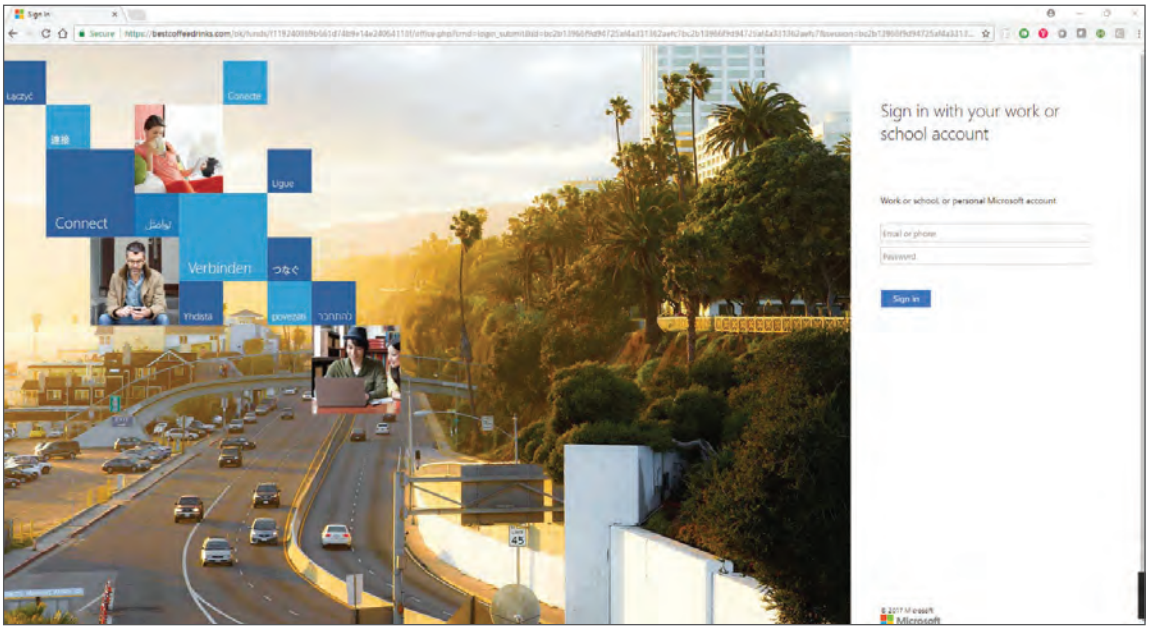

Figure 7: bestcoffeedrinks.com Displays a Microsoft Authentication Page

This site has multiple, different login pages including:

- DocuSign: well-known service for signing documents
- Wells Fargo: international banking and financial services holding company
- Microsoft: software and services for both personal and business use

What are these doing on a site named bestcoffeedrink.com? A cybercriminal created these to steal credentials as part of a phishing attack. They would send phishing emails on behalf of DocuSign, or Wells Fargo, or Microsoft with the links to the appropriate login pages on this site. Users are busy and some will forget to check the name of the site against the login prompt and be hooked.

Misdirection 1: The web page is a simple login screen requesting email credentials with a promise "to access shared files and folders."

Misdirection 2: The inclusion of a choice of email providers — Gmail, Yahoo, Hotmail, or AOL. These login and verification pages are (we know) obviously fake and if you click on the "Login" or "Continue" button without entering an email, password, or phone number, they will still work. The only purpose of these fake pages is to draw out your confidential data.

Misdirection 3: The site uses a valid SSL certificate of type DV, causing web browsers to display a green lock icon with the "Secure" keyword. This also helps trick the users into thinking it is safe and secure to access this page.

Getting a single web domain to host different web pages is easy. Just place each page under different folders. See *Figure 8: Directory Structure of bestcoffeedrinks.com* for this site's layout.

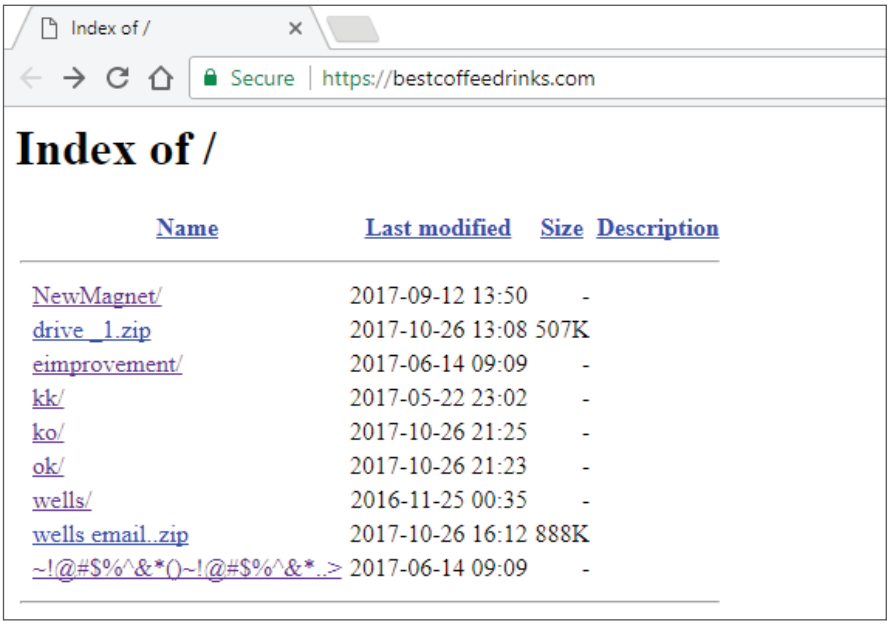

Figure 8: Directory Structure of bestcoffeedrinks.com

Each different folder contains a copy of a different website. In this case, some are invalid pages — a sign of the cybercriminal testing as they went. Once a domain is compromised, any resource may be dumped here and used for malicious intent.

How to Defend Against Phishing Attacks

When it comes to phishing, knowledge is your most powerful defense. When accessing the web remember: your carelessness is the best instrument for a cybercriminal and your awareness is his or her worst enemy.

The Comodo Threat Intelligence Lab recommends the following to protect you and your organization:

- Were you expecting an email attachment? If not, check back with the sender before opening it.
- Compare the domain name in a browser address bar carefully with the content on the page — do they match?
- Never click on unverified links in an email. Instead try copying the link into a text editor to see what the actual link goes to.
- Be wary of unexpected emails purportedly from your company's scanner/copier (see *Figure 9: Sep 2017 Phishing Email Pretending to Come From a Copier*).
- When downloading software, especially freeware, make sure you type in the corporate website rather than clicking on a link in an email.
- Make sure your endpoint protection solution enables a "default-deny" security posture for unknown files (including auto-containment of unknown files while they're being analyzed to see if they are malware).

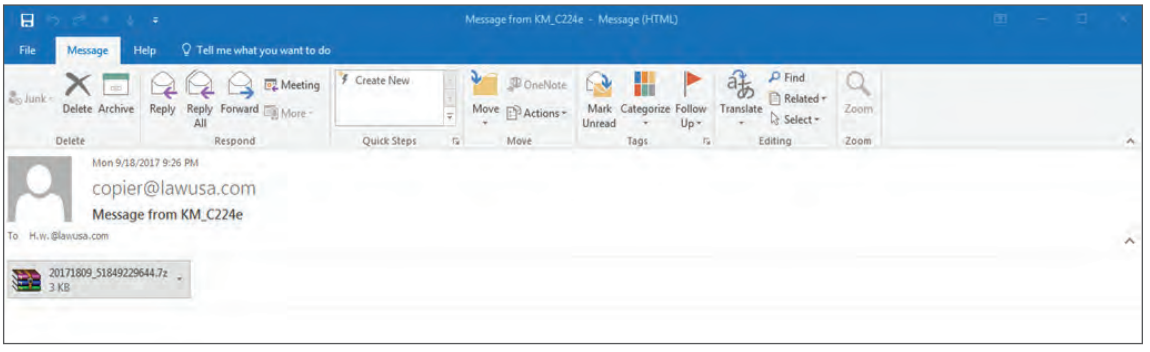

Figure 9: Sep 2017 Phishing Email Pretending to Come From a Copier

Consider Comodo tools and all the Comodo Threat Research Labs as your partner to create an effective barrier against phishing attacks — Comodo offers “defense-in-depth” cybersecurity protection. The Comodo Threat Intelligence Lab is a valuable supporting resource and in modern cyberspace, knowledge provides the real power to survive.

These special reports from the Lab (as well as other reports and updates) are available to subscribers of Comodo Threat Intelligence Lab Updates.

Subscribe for free at: comodo.com/lab

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.
For more information, visit comodo.com.

Keep up to date with the Latest Comodo News:
Blog: *https://blog.comodo.com/*
Twitter: *@ComodoNews*
LinkedIn: *https://www.linkedin.com/company/comodo*

About The Comodo Threat Intelligence Lab

The Comodo Threat Intelligence Lab (the Lab) monitors, filters and contains, and analyzes malware, ransomware, viruses and other "unknown" potentially dangerous files 24x7x365 in over 190 countries around the world. With 5 offices spread across the Americas, Asia and Europe (and staff covering over 190 countries), the Lab is made up of more than 120 IT security professionals, ethical hackers, computer scientists and engineers (all full-time Comodo Lab employees) analyzing millions of potential pieces of malware, phishing, spam or other malicious/unwanted files and emails every day. The Lab also works with trusted partners in academia, government and industry to gain additional insights into known and potential threats.

The Lab is a key part of the Comodo Threat Research Labs (CTRL), whose mission is to use the best combination of cybersecurity technology and innovations, machine learning-powered analytics, artificial intelligence and human experts and insights to secure and protect Comodo customers, business and public sector partners and the public community.

Comodo Group, Inc. | 1255 Broad Street, Clifton, NJ 07013 US
Tel: +1 (888) 266-6361 | Tel: +1 (703) 581-6361 | Fax: +1 (973) 777-4394