Tricky Forms of Phishing

By Paul Miguel Babon (words)

Published: 2020-09-03 · Archived: 2026-04-06 03:19:52 UTC

The internet has long been an indispensable tool for various industries, all the more so now with the current pandemic, as many companies rely on internet connectivity for powering work-from-homenews article setups. Unfortunately, cybercriminals capitalize on the usability of the internet to extort users. One of the most common means to do this is through phishing.

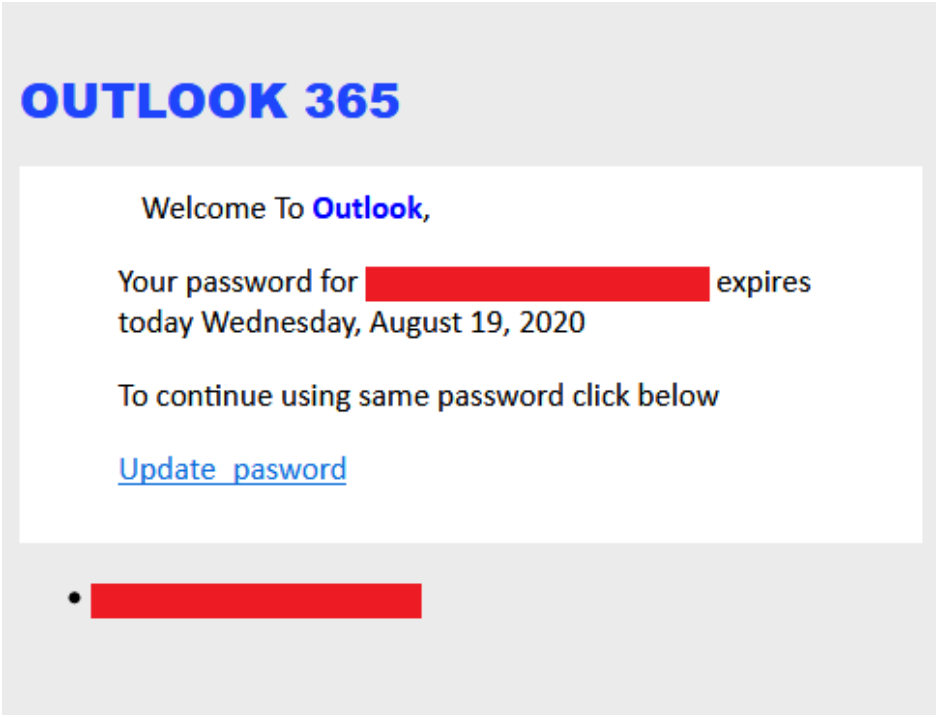
Phishing schemes are served by websites that harvest sensitive information such as credit card numbers, social security numbers, and account credentials, among others. Many of these are hosted on websites with spoofed domainsnews-cybercrime-and-digital-threats or pages created through website builders. Recently, however, creating phishing pages has become even easier through the use of forms — tools that can be configured within only a few minutes.

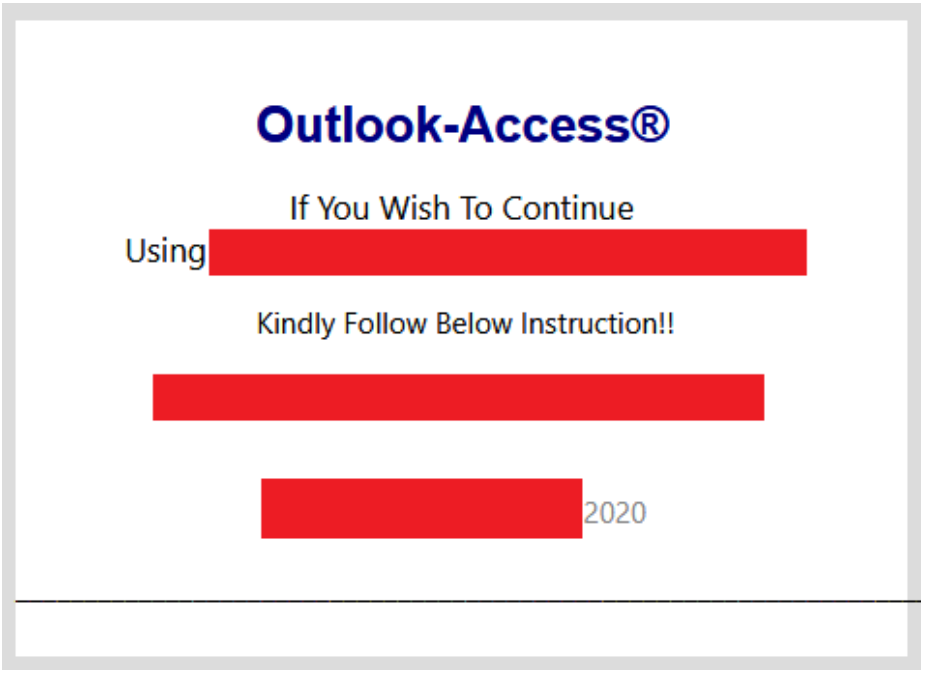
How are these schemes formed?

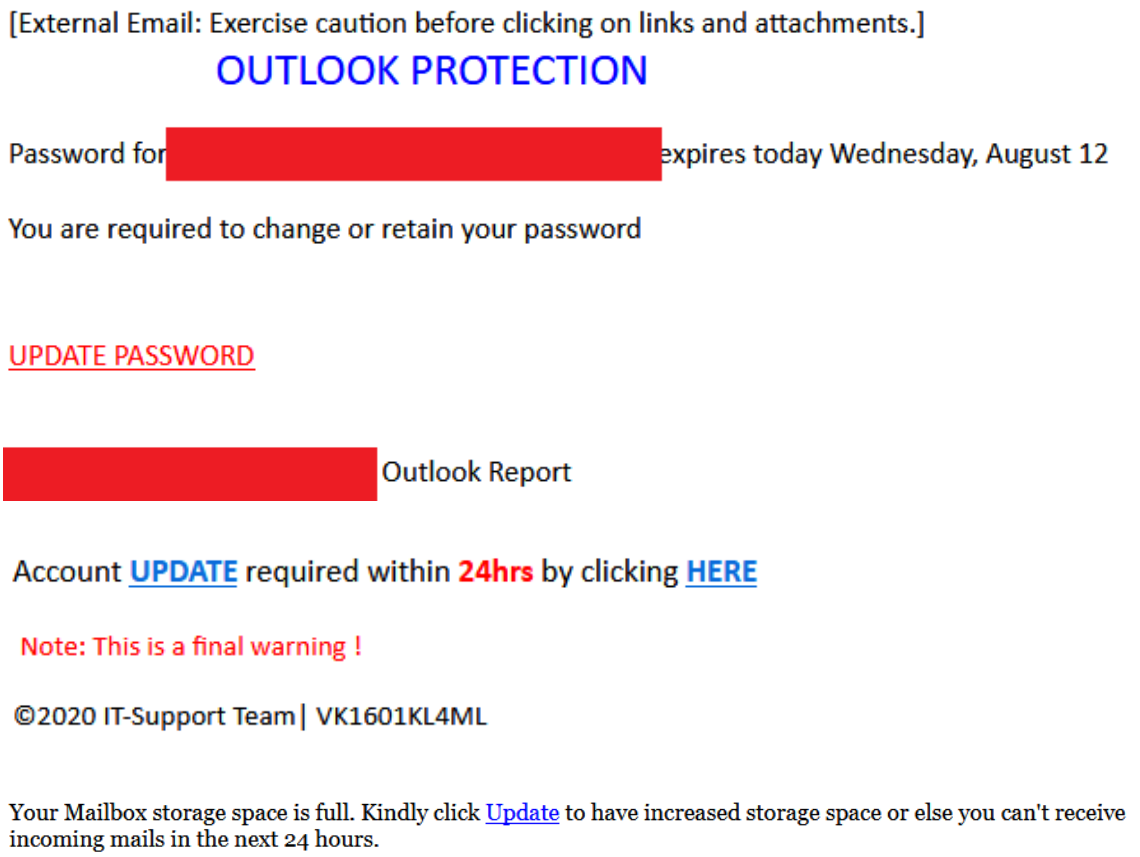
Here are common examples of form builder services that are used to create forms for phishing. Notably, on their own, they are legitimate, non-malicious sites. However, like other legitimate platforms, they can also be exploited:

- 123formbuilder.com
- docs.google.com
- form.simplesurvey.com
- formpl.us
- forms.gle
- forms.office.com
- formtools.com
- smartsurvey.co.uk
- supersimplesurvey.com
- survey.survicate.com
- surveygizmo.com
- survs.com
- zfrmz.com

Within a few minutes and even without programming knowledge, cybercriminals can create forms in these sites. These pages are then propagated through emails, like in most phishing campaigns. Some examples of these are emails that pose as advisories from Microsoft Outlook, which prompt the user to open a link to update a supposedly expiring password or full mail storage. A common form builder used for these emails is Microsoft Forms, perhaps to enhance believability since this site is also from the same vendor as Outlook. Super Simple Survey is commonly used as well.

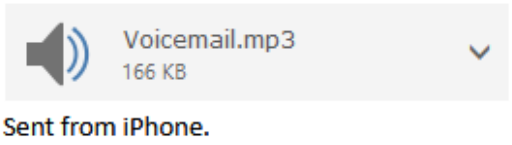

OUTLOOK 365
Welcome To Outlook,
Your password for [redacted] expires today Wednesday, August 19, 2020
To continue using same password click below
Update pasword
•

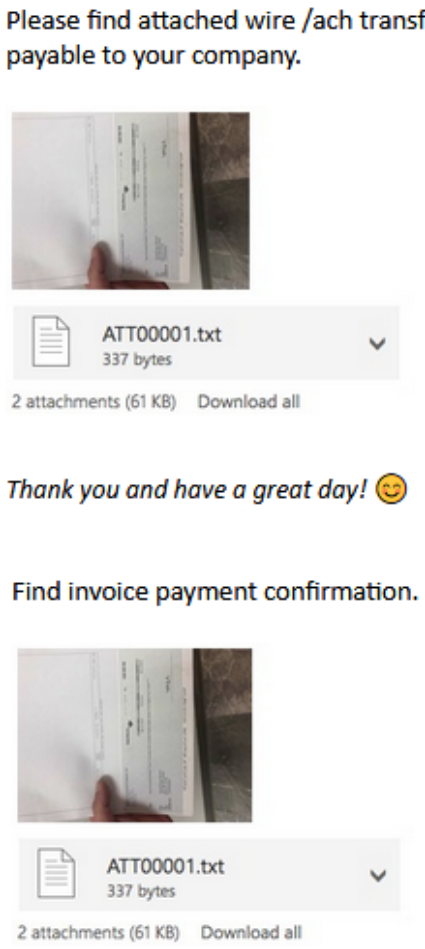

Outlook-Access®
If You Wish To Continue
Using [redacted]
Kindly Follow Below Instruction!!
[redacted]
[redacted] 2020



Figures 1-5. Phishing emails posing as advisories from Microsoft Outlook

Some cybercriminals also pose as business representatives in their emails and mask phishing links as fake voicemails or documents. We observed Survey Gizmo being commonly used for these.



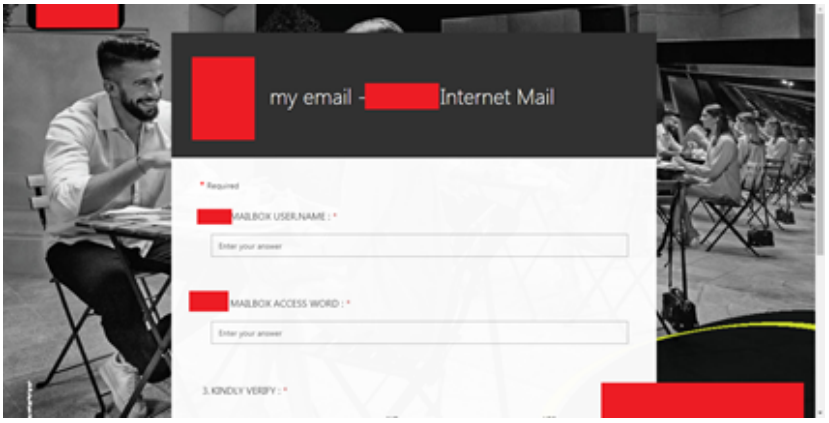


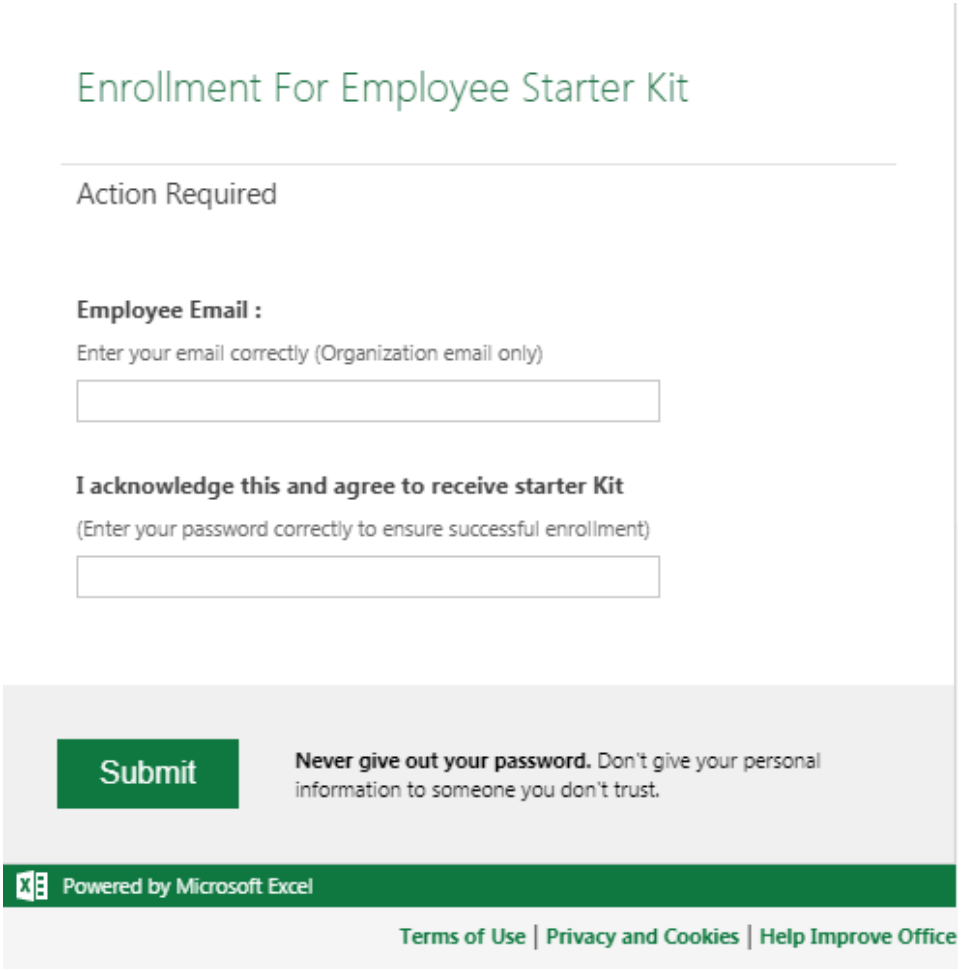
Figures 6-8. Phishing emails with a fake voicemail and document attachments

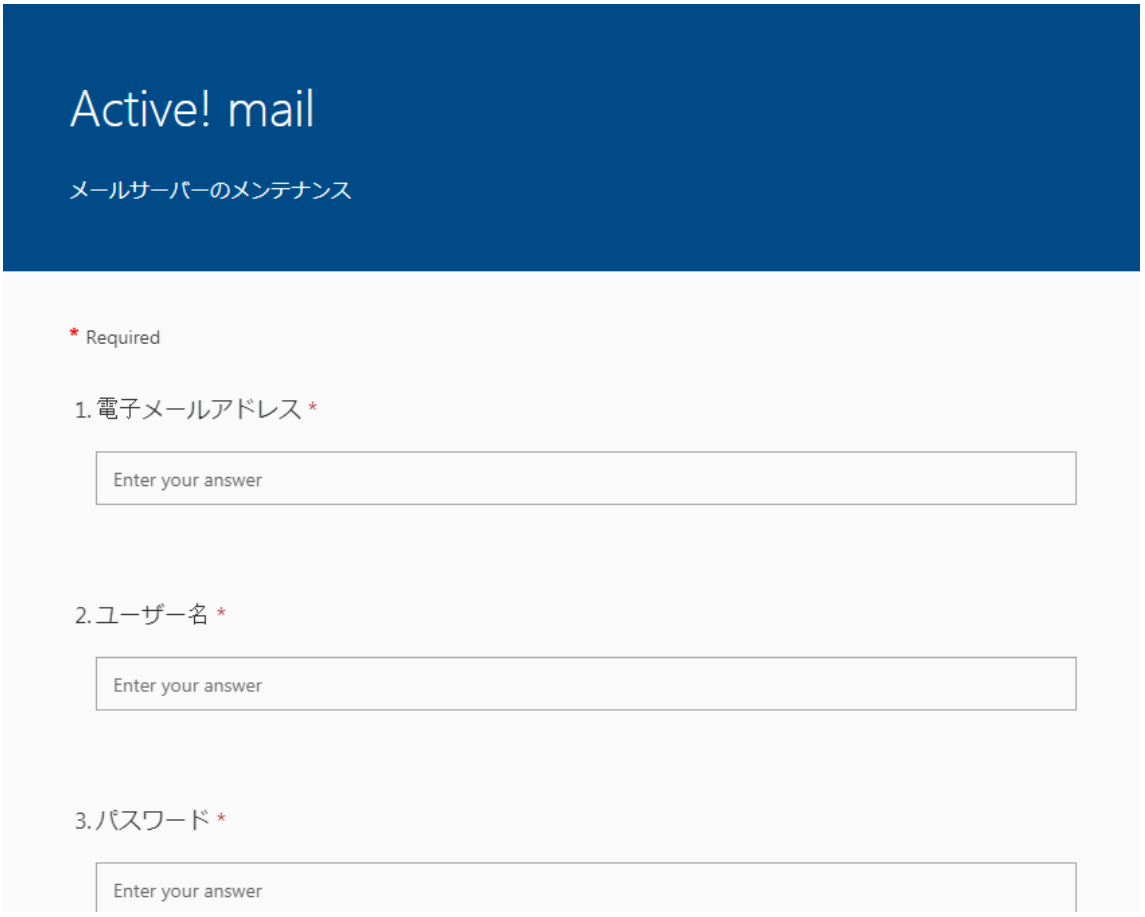
Selecting the buttons, a fake voicemail, or a document in these emails redirects the users to phishing sites that are housed on these forms.

Figures 9-10. Examples of phishing links housed in form builders

Like other phishing sites, these forms attempt to harvest information such as email addresses and passwords. They can pose as email login or verification pages.

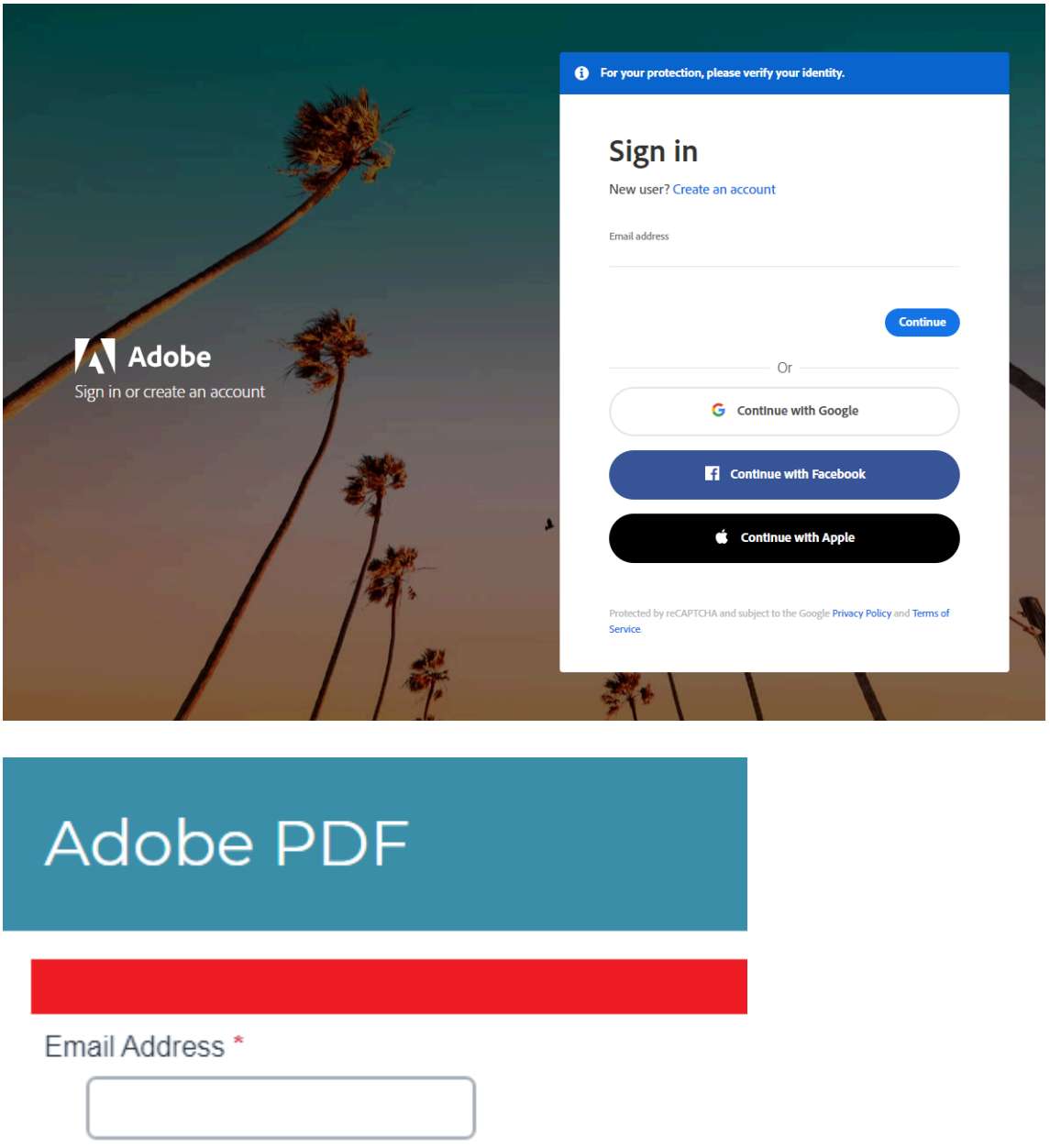

my email - Internet Mail
* Required
MAILBOX USER.NAME : *
Enter your answer
MAILBOX ACCESS WORD : *
Enter your answer
3. KINDLY VERIFY : *


Enrollment For Employee Starter Kit
Action Required
Employee Email :
Enter your email correctly (Organization email only)
I acknowledge this and agree to receive starter Kit
(Enter your password correctly to ensure successful enrollment)
Submit
Never give out your password. Don't give your personal information to someone you don't trust.
Powered by Microsoft Excel
Terms of Use | Privacy and Cookies | Help Improve Office

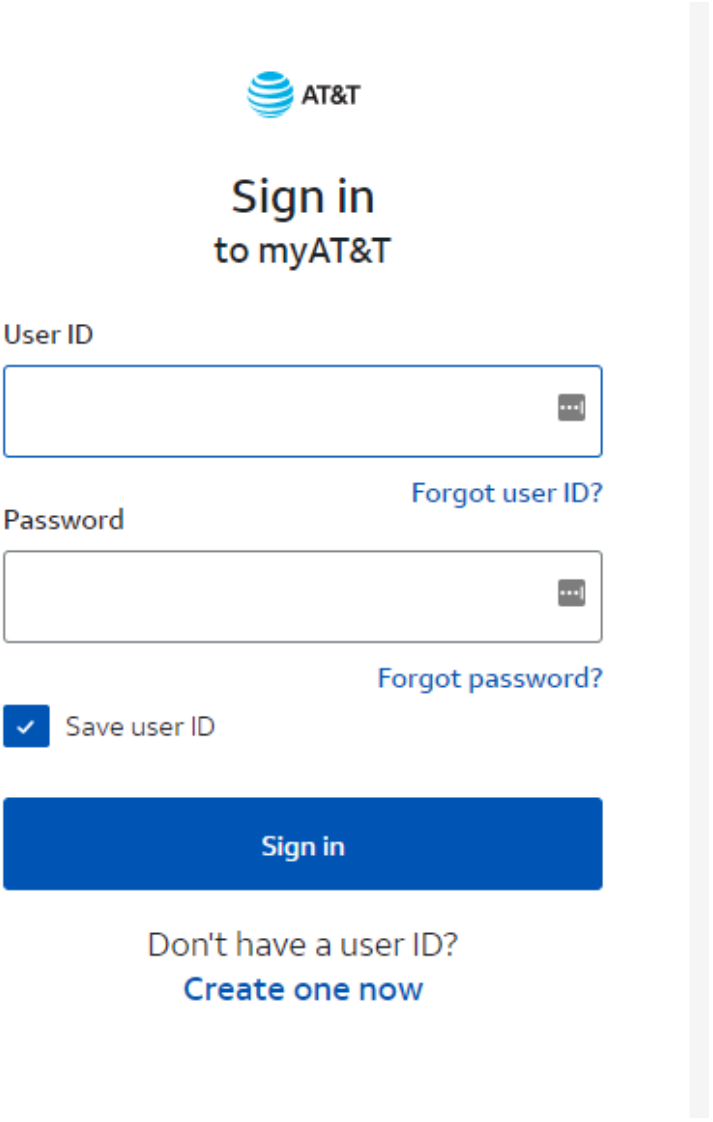


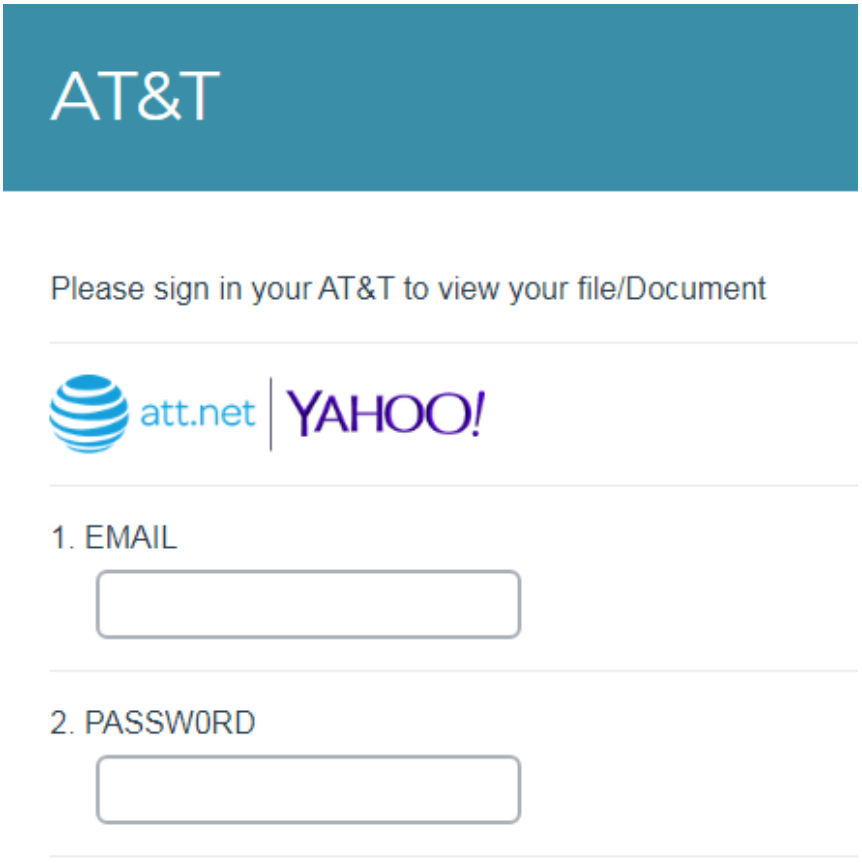
Figures 11-13. Examples of forms that were made for phishing

It is relatively easy to spot the differences between a real login page and one made with a form as the latter looks templated and blocky. However, users might still erroneously trust a site if they see that a legitimate website (such as the form builder site) is associated with it.

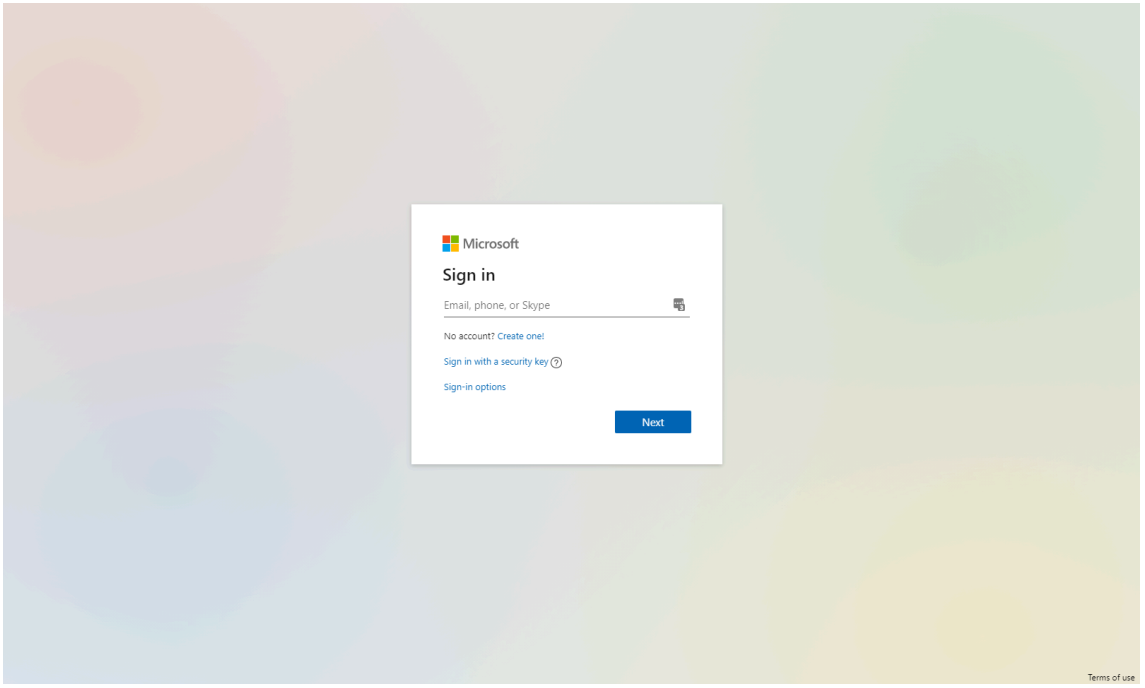


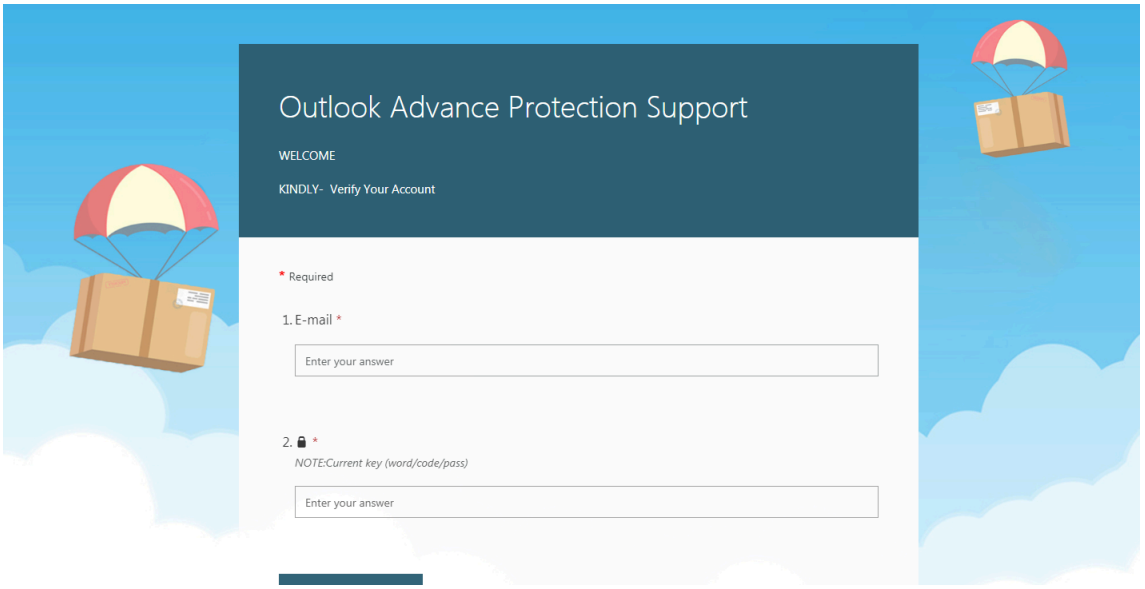
Figures 14-15. Top: Legitimate Adobe login page. Bottom: Fake Adobe login page made of a form


AT&T
Sign in
to myAT&T
User ID
Forgot user ID?
Password
Forgot password?
Save user ID
Sign in
Don't have a user ID?
Create one now



Figures 16-17. Top: Legitimate AT&T login page. Bottom: Fake AT&T login page made of a form





Figures 18-19. Top: Legitimate Microsoft Outlook login page. Bottom: Fake Microsoft Outlook login page made of a form

What makes form builders a viable option for cybercriminals?Other than form builders, phishing authors commonly use fake domains and website builders to create phishing pages. This table details a side-by-side comparison of all three, the reasons that form builders are an attractive option, and ways that users can spot these sites:

	Fake Domains	**Website Builders**	**Form Builders**
Definition	The creation of a new domain where the name and the appearance of a popular website are copied. This is used to fool people into thinking that they are on the right website.	The use of site creation services like wix.com or weebly.com. These services offer convenience in creating professional-looking phishing pages, some of which can look like popular websites.	The abuse of forms services like Microsoft Forms to create simple and fake phishing pages and sometimes even fake login pages
Examples	amaazoon[.]xyz go0gle[.]fun	outlookmail[.]weebly[.]com googledrivefiles[.]wixsite[.]com	forms[.]office[.]com/Pages/ResponsePage.aspx?id=rand0mnU docs[.]google[.]com/forms/d/e/rand0mnU

Creation Difficulty	Requires knowledge of programming and web hosting to create the website	Requires some knowledge of HTML programming as well as design skills to make the phishing website convincing	Requires only basic knowledge of how forms are made
Resources	Requires lots of time to set up. Money is also involved in buying domains, making this tactic resource-intensive.	A decent amount of time is needed to create a professional-looking website. Some services require money to create websites, some do not. Still, some phishing authors would rather use this tactic than create fake domains from scratch.	Small-to-little amount of time is needed to create a phishing page. A person can easily create one in minutes. Usually, depending on the service, money is not needed to create a form. This is advantageous for phishing authors as they can create loads of phishing forms.
How Users Can Spot These	By thorough inspection of the URL to detect whether the website is legitimate	By spotting the domain "weebly[.]com" or "wix[.]com" instead of the original domain in the address bar	By keeping in mind that companies usually do not use forms for password updates or email verification

Conclusion

In our 2020 midyear security roundup, we reported our detection of nearly 7 million unique phishing URLs for the first half of 2020, a 28% increase in over 5 million detected URLs in the second half of 2019. This shows that phishing remains a favorite weapon among cybercriminals. Similar to the case of other threats, operators behind these schemes find ways to spend both less time and money to enable their scam while also ensuring that it remains effective, if not more formidable. From creating websites from scratch, operators eventually progressed to creating pages from website builders. Today, they also use forms.

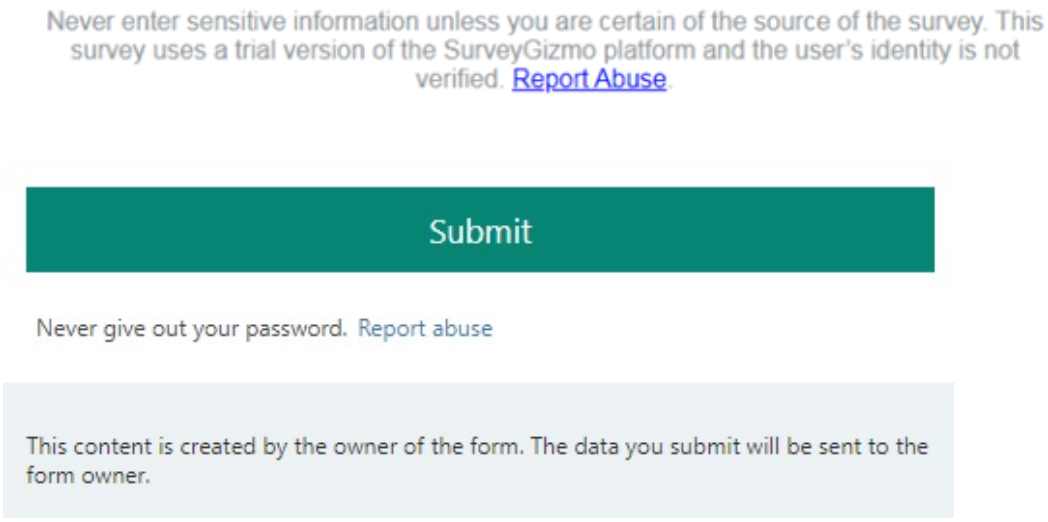
Forms can be created in a few minutes, usually do not cost a cent, and can pass off as professional — at least at the basic level. Some users tend to trust them as well since the form builder websites themselves are not malicious, and sometimes the domains are related to the information requested by the phishing website (for example, a Microsoft Forms page used to harvest Microsoft account credentials). Therefore, these forms can do the job with little work required.

As the tactics used by cybercriminals evolve, users can defend themselves by thoroughly inspecting pages (whether websites or forms) that request for credentials. Security solutions can also help detect and block these threats.

Forming strong defenses against phishing

Users can protect themselves from forms used for phishing by following these specific steps:

- Never give out passwords and other sensitive information. Forms and surveys are used for responses, opinions, feedback, and application purposes — they are not a substitute for login pages.
- Report phishing forms immediately. If a form requires the user to fill in credentials and other sensitive information, report it to the form builder service itself. The links to report the form are usually located at the bottom portion of the page:



Figures 20-21. Sample portions of forms for reporting abuse.

- Always double-check if the email sender is legitimate. Do not open any links if the sender is unknown or suspicious.
- If there is a suspicious email, report it to your company's InfoSec or IT Security team.
- Ensure that the security settings of all applications are up to date.

The following security solutions are recommended as a defense against phishing:

- Trend Micro™ Cloud App Securityproducts – Enhances the security of Microsoft Office 365 and other cloud services. It uses computer vision and real-time scanning to find credential-stealing phishing sites. It also protects against business email compromise (BEC) and other email threats.
- Trend Micro™ Deep Discovery™ Email Inspectorproducts – Defends users against phishing and ransomware attacks through real-time scanning and advanced analysis techniques for known and unknown attacks.

The internet is a vast, open world full of doors to opportunities for achieving a convenient lifestyle. With that being said, it is crucial to be conscious of the fact that these doors can also lead to abuse and baits. Therefore, we must always take steps to protect our data and not take its security for granted.

Tags
