Email is the number one threat vector. There's no exception, even with a global pandemic. On the contrary: Covid-19 has been used as an appealing hook by cybercriminals. Data from Trend Micro Smart Protection Network shows that for the first five months of 2020, 92% of all the cyberthreats leveraging Covid-19 were spam or phishing email messages.

Are employees the weakest link in your security strategy?
Email scams can have a big impact, on both the organization and the individual. This was highlighted in a recent report from BBC News where a finance professional from Glasgow, Scotland was targeted by a business email compromise (BEC) scam. The hackers disguised themselves as the employee's CEO and managed to convince her to transfer 200,000 British pounds (approximately US$261.95 as of writing) to their bank account. When the organization realized what happened, they were able to retrieve half of the loss. However, the employee was fired and then pursued in the courts for the remaining sum. Her lawyers argued successfully that she had not received any training to identify these scams and the case was subsequently dismissed.

This took a big personal toll on the employee who not only lost her job, but worried about losing her home as well. Her employer suffered financially and their reputation also took a hit. There were no winners in this case, but it really emphasized the importance of security awareness; companies need to arm their employees with the knowledge to protect the business and ultimately, themselves.

A great email security solution can block the majority of threats, but no product can catch a hundred percent of email scams. This means that humans are our last line of defense.

Want to train your organization?

Trend Micro™ Phish Insight service helps you to increase your employees’ awareness of phishing emails and other cyberthreats. Best of all, it is completely free, allowing you to increase your cybersecurity while using this budget for other critical initiatives.

To start a phishing simulation for your users, you need zero budget and only five minutes. With a simple user experience, you can get up and running with your first simulation today. Try Phish Insight with no obligation.

To see how a US company was able to use Phish Insight to successfully increase employees’ awareness while being able to target more at-risk user groups and identify those that need more help, click here.

Tricky 'Forms' of Phishing

The internet has long been an indispensable tool for various industries, even more so now with the current pandemic, as many companies rely on internet connectivity for powering work-from-home 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 domains 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?

Form builder services 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. Some examples include 123formbuilder.com, docs.google.com, and form.simplesurvey.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.

Some cybercriminals also pose as business representatives in their emails and mask phishing links as fake voicemails or documents. Selecting the buttons, a fake voicemail, or a document in these emails redirects the users to phishing sites that are housed on these forms.

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.
Examples of forms that was 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.

Left: Legitimate Adobe login page. Right: Fake Adobe login page made of a form

Conclusion

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:
Sample portion 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 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.

*Note: You may also view this newsletter on https://internetsafety.trendmicro.com/business/resources*