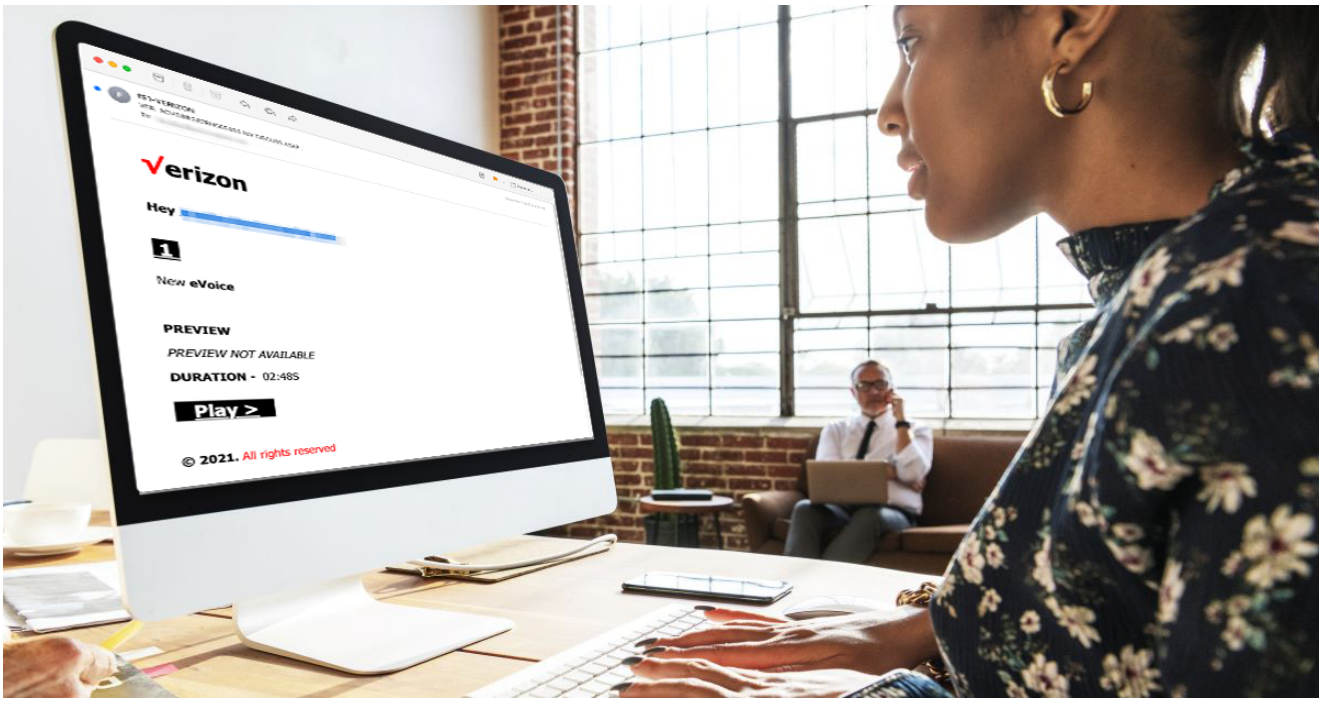
Fresh Phish: Phishers Get Clever, Use Math Symbols for Verizon Logo

inky.com/blog/phishers-get-clever-use-math-symbols-for-verizon-logo



Posted by Roger Kay

- Tweet
-

A large category of phishing attacks comes under the heading of brand impersonation. The idea is to fool an email recipient into interacting with what they think is a known and trusted brand. Recently, data analysts at INKY began to see a pattern of attacks impersonating Verizon, the large U.S.-based telecommunications provider. What made these attacks interesting was their use of mathematical symbols as part of the Verizon logo.

Despite all the money major brands spend on logo design, people are terrible at remembering them. This fluke of human nature plays well into the hands of phishers, who can deceive their victims with made-up logos that look about right. Their graphics may be off, but they do the job. It probably helped the phishers that Verizon has changed its logo a couple of times since Bell Atlantic Corporation was renamed Verizon in 2000.

INKY, which provides anti-phishing technology, detected this Verizon impersonation campaign in dozens of fake emails sent from various Gmail addresses during a two-week period between September 1-13, 2021.

Quick Takes: Attack Flow Overview

- Type: phishing
- Vector: several “freemail" accounts, newly created web domain
- Payload: malicious link to credential harvesting site
- Techniques: brand impersonation
- Platform: Office365
- Target: Microsoft users

The Attack

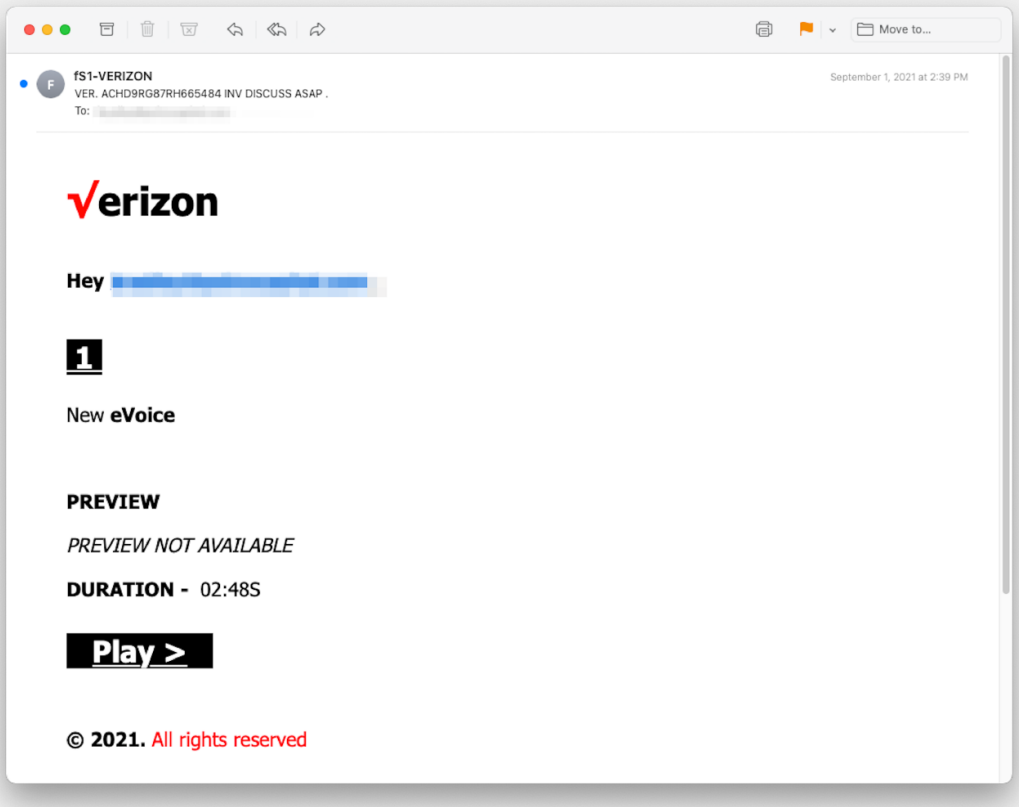
Although Verizon's current logo makes use of a bright red, asymmetrical “V” after the word “Verizon” (which is all lower case in bolded black sans serif), that "V" element does look rather like a checkmark.

The real Verizon logo

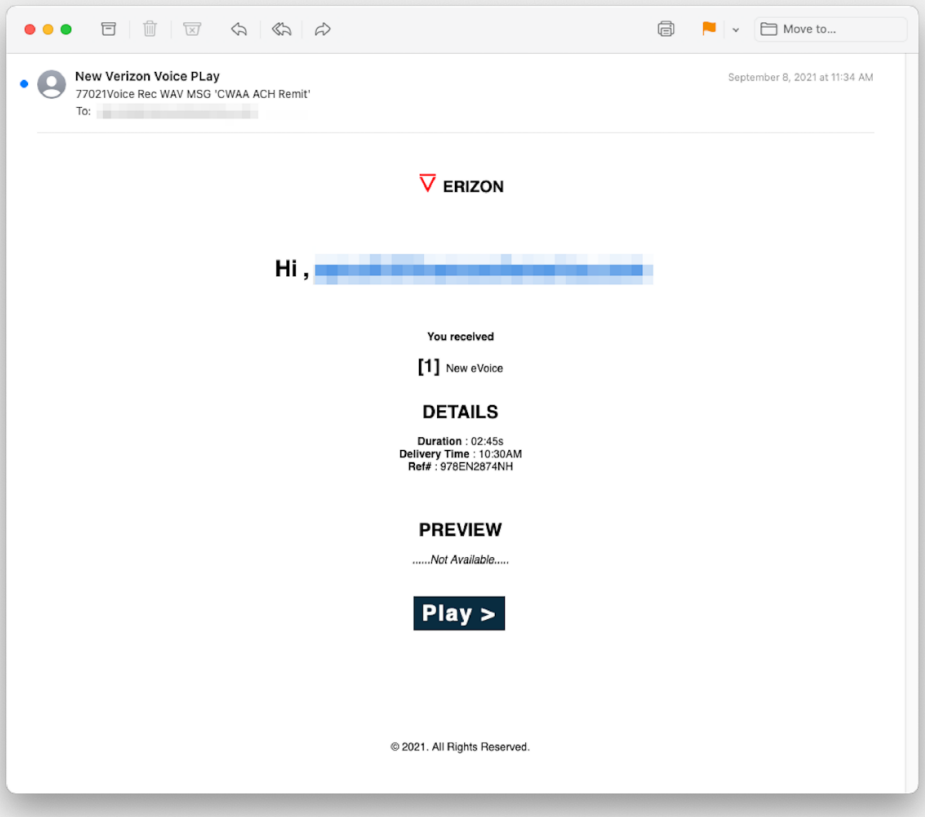
INKY found three fake logo variants in the wild. Each made use of a mathematical symbol for the red element. The three impersonations reproduced that element via:

- a square root symbol,
- a logical NOR operator, and
- the checkmark symbol itself.

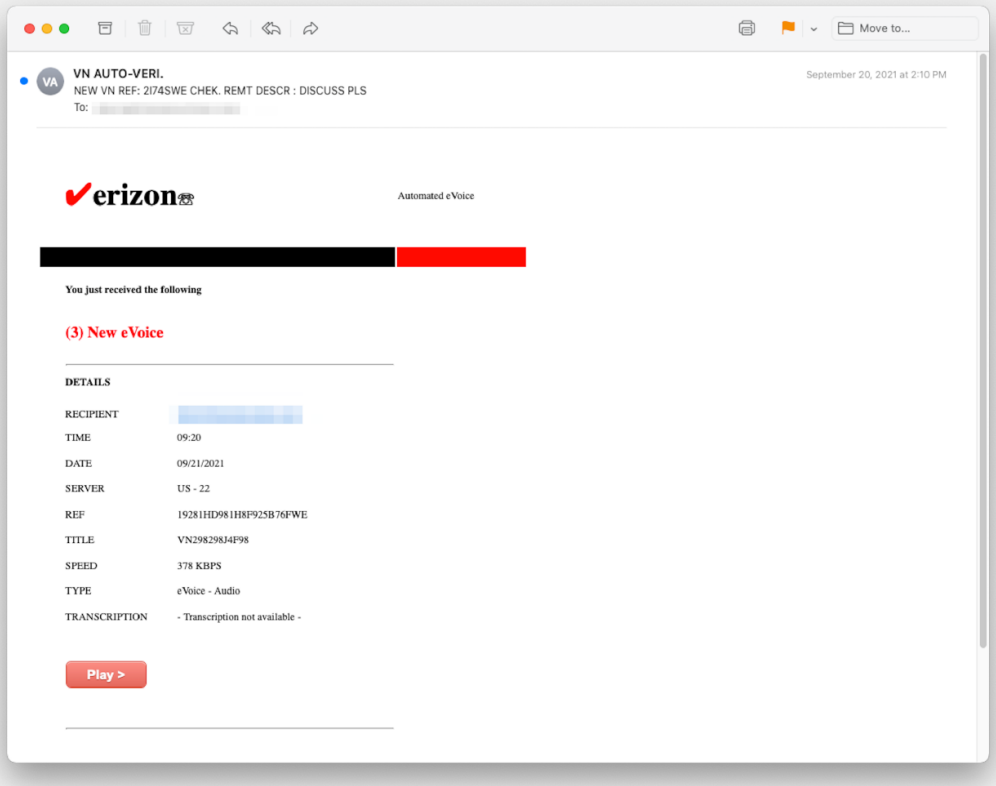
Sample emails are shown below.



The square root symbol √ stood in for the "V" in Verizon



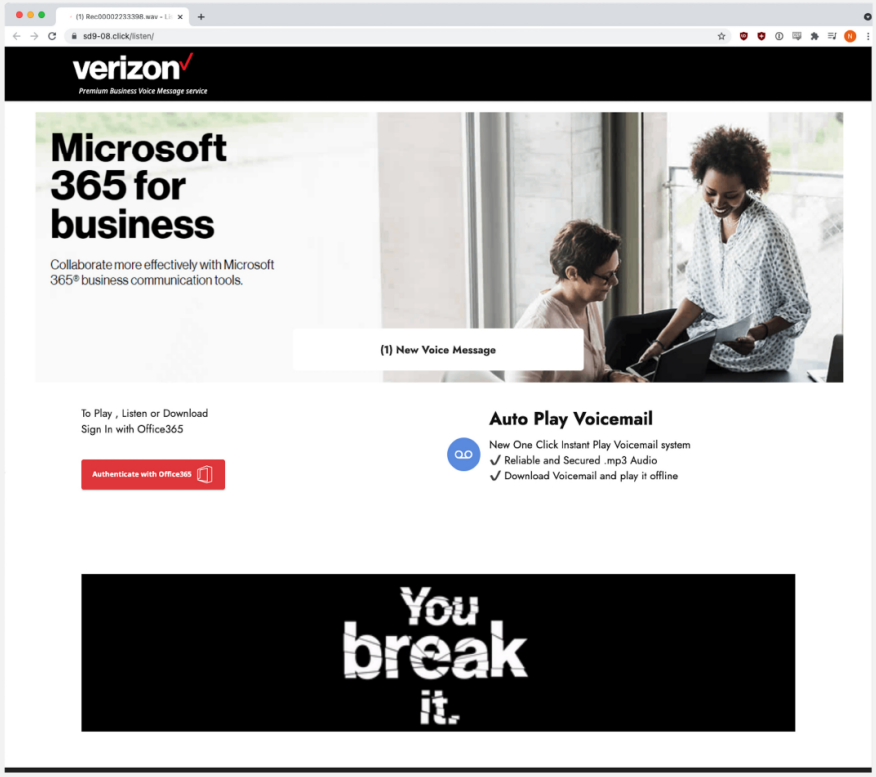
The "V" in Verizon was depicted by a Boolean NOR operator



Rather than following the brand name, as it does in the real logo, the check mark symbol was substituted for the "V" in Verizon

All three types masqueraded as voicemail notifications. Verizon does provide voicemail services, including notifications.

Clicking on the button (black or red, depending on the version) prominently displaying the text "Play >" (made up of the word plus a close-angle-bracket character) led to a site that appeared to be Verizon's, but was in fact a malicious impersonation. The phishers were easily able to steal separate HTML and CSS elements from Verizon's real site to put together a custom job that included a correct version of the logo!



Not Verizon, despite the correct logo

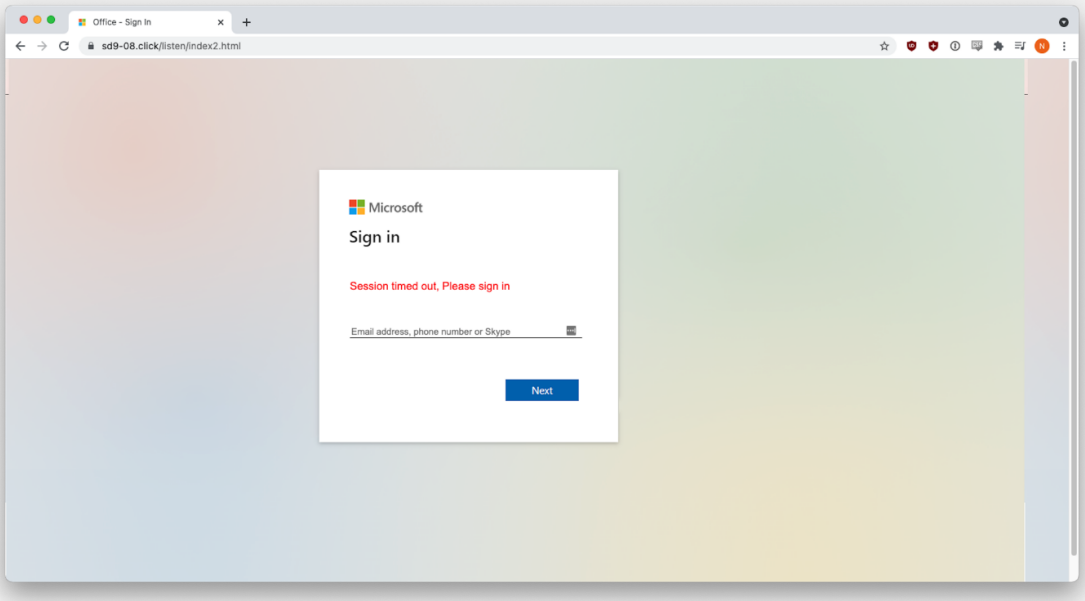
The bad guys created and registered the fake site — `sd9-08[.]click` — via Namecheap barely a month ago, according to a WHOIS lookup. Namecheap has since taken it down. It now has an NXDOMAIN status, which essentially means it doesn't exist anymore.

```
# whois.namecheap.com

Domain name: sd9-08.click
Registry Domain ID: DO_8c23c47a623ab1d3411dc391d877c05e-UR
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2021-09-01T16:46:50.29Z
Registrar Registration Expiration Date: 2022-09-01T16:46:50.29Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
```

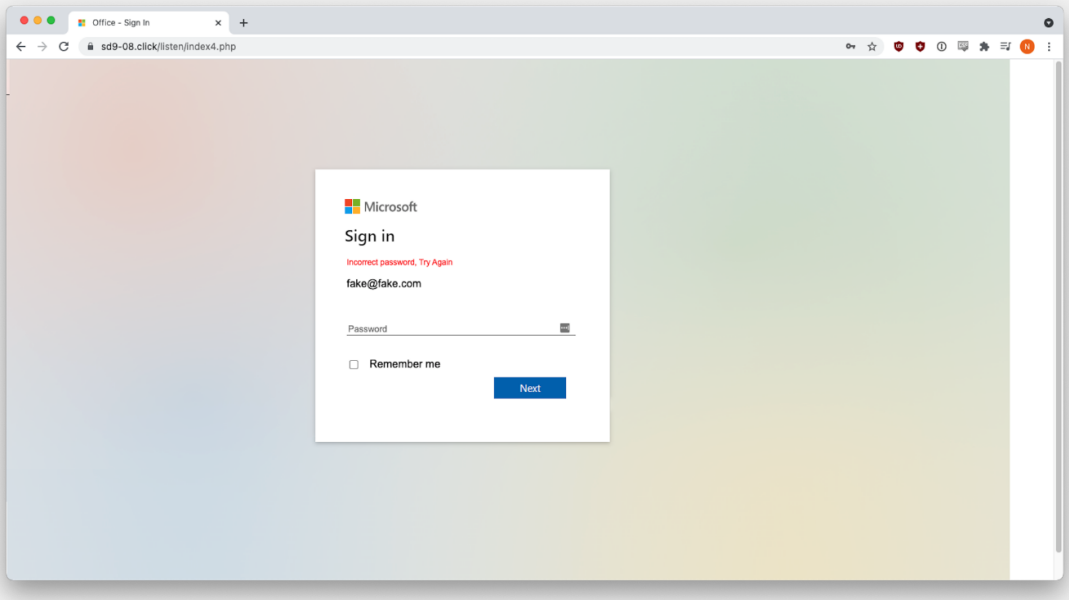
The malicious site registration

At the bottom of the fake page, targets were invited to “play, listen, or download” their voicemail with Office365 credentials. Using the red “Authenticate with Office365” button led to a fake Microsoft login dialog box.



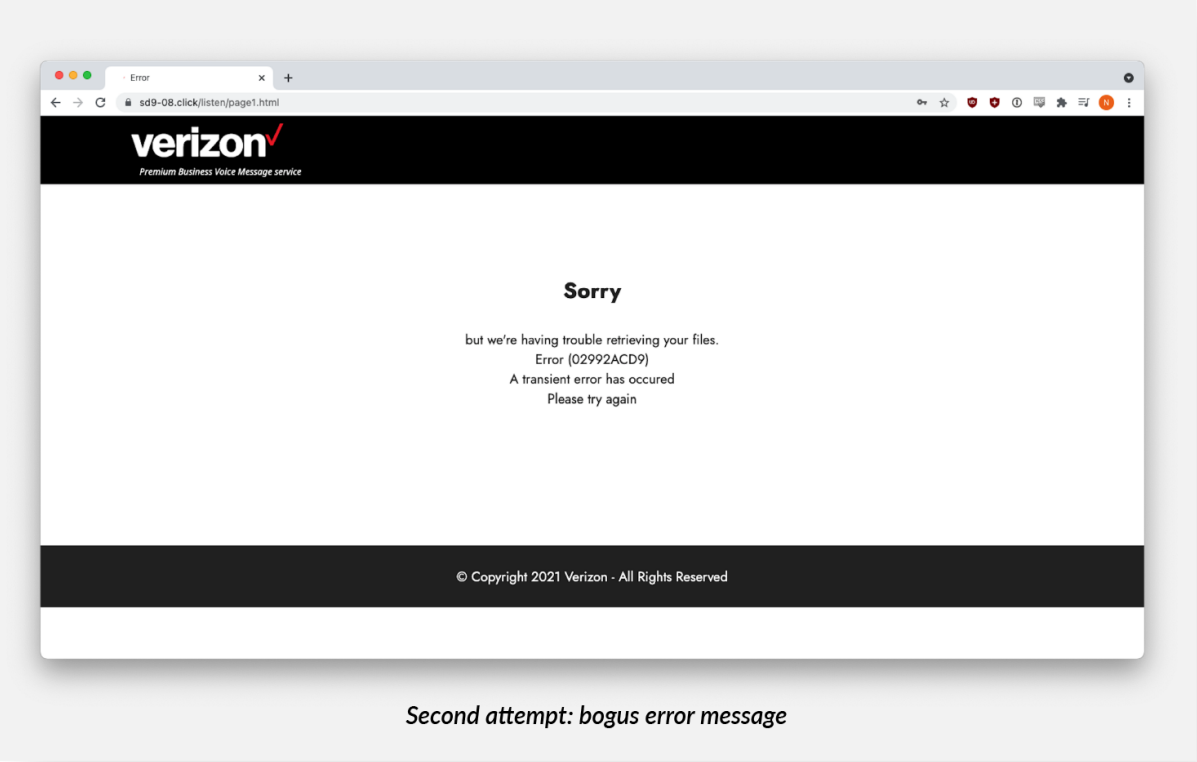
Fake Microsoft login

An INKY analyst entered fake credentials into the fake login to assess the site.



First attempt: incorrect password

The first attempted login received a response that the password was incorrect. The second attempt elicited a bogus error message.



Second attempt: bogus error message

However, the credentials were harvested both times on the backend. This pattern, the double ask, is fairly common. It's not entirely clear what the phishers are up to, but it's possible that they want the victim to confirm the correctness of the data, or that they hope the victim will try a different account, yielding them two sets of credentials for the price of one.

Techniques

The phishers sent phishing emails from Gmail accounts because they were able to pass standard email authentication (SPF, DKIM, and DMARC). The malicious site was brand new and presented zero-day vulnerabilities; they had never been seen before and did not appear in threat intelligence feeds commonly referenced by legacy anti-phishing tools. Without a blemish, this site did not look malicious.

Recap of Techniques:

- Brand impersonation — uses brand elements, in this case Verizon's, in phishing emails and a malicious site, which also impersonated Microsoft brand elements
- Credential harvesting — occurs when a victim tries to log into what they think is a real Microsoft site but enters credentials into a form controlled by the phishers
- Newly created domains — are used by phishers to pass most security software tests, allowing phishing emails to slip past corporate defenses and into hapless recipients' inboxes

Best Practices: Guidance and Recommendations

Email recipients are advised to be suspicious of voicemail notifications coming from Gmail or other free email providers such as Yahoo, AOL, or Hotmail. They should also distrust emails that claim to be from Verizon but come from a Gmail sender.

Also, in many cases, they can look at the URL of a site that purports to be Verizon to see whether Verizon actually hosts it. This type of analysis will sometimes lead to false positives if a large company uses a smaller firm for marketing support.

They should also be wary if a site asks them to enter Microsoft credentials to view notifications from Verizon (or any other brand).

INKY reported this flurry of phish to Verizon's phishing@verizon.com address. Although this particular campaign is over, anyone receiving a similar email in the future can report it to that address with their name and account, and phone numbers. Verizon also sent INKY a link to a general security question page, where the company addresses the broader scam landscape.

Fresh Phish examples were discovered and analyzed initially by Bukar Alibe, Data Analyst, INKY

This article is part of our Fresh Phish series, featuring some of our most interesting phish caught by INKY.

About INKY

Headquartered in College Park, Maryland, INKY leads the industry in mail protection powered by unique computer vision, artificial intelligence, and machine learning. The company's flagship product, INKY Phish Fence, uses these novel techniques to "see" each email much like a human does, to block phishing attacks that get through every other system. INKY founder Dave Baggett also co-founded ITA Software, the industry-leading airfare search company purchased by Google in 2011 for $730M, which now powers Google Flights®. For more information, please visit https://INKY.com/.