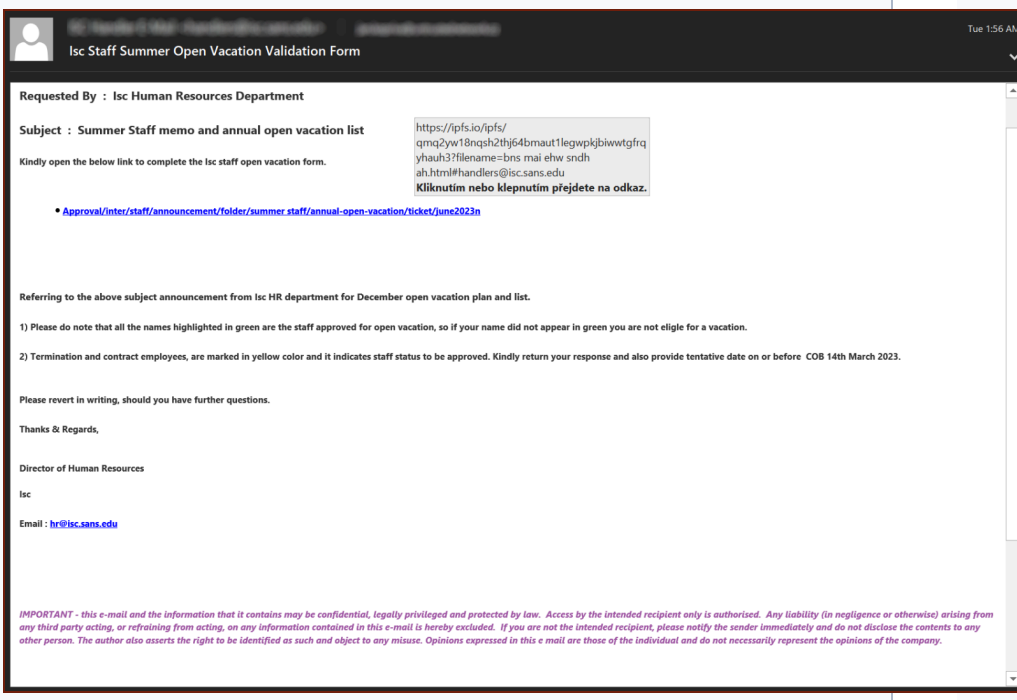
IPFS phishing and the need for correctly set HTTP security headers

Published: 2023-03-15. **Last Updated**: 2023-03-15 11:22:07 UTC
by Jan Kopriva (Version: 1)

0 comment(s)

In the last couple of weeks, I've noticed a small spike in the number of phishing messages that carried links to fake HTML login pages hosted on the InterPlanetary File System (IPFS) – an interesting web-based decentralized/peer-to-peer data storage system. Unfortunately, pretty much any type of internet-connected data storage solution is used to host malicious content by threat actors these days, and the IPFS is no exception. In fact, it seems to have been used to host phishing pages since at least the beginning of 2022[1].

social engineering techniques it uses. What makes it somewhat interesting, besides the fact that it depends on IPFS, is that it also shows quite nicely the need for organizations to ensure that security-related headers are set by their web servers. This is because although, as you may see from the examples shown below, all the e-mails linking to pages hosted on IPFS were different...



Isc Staff Summer Open Vacation Validation Form

Requested By : Isc Human Resources Department

Subject : Summer Staff memo and annual open vacation list

Kindly open the below link to complete the Isc staff open vacation form.

https://ipfs.io/ipfs/qmq2yw18nqsh2thj64bmaut1legwpkjbiwwtgfrqyhauh3?filename=bns mai ehw sndh ah.html#handlers@isc.sans.edu
Kliknutím nebo klepnutím přejdete na odkaz.

• Approval/inter/staff/announcement/folder/summer staff/annual-open-vacation/ticket/june2023n

Referring to the above subject announcement from Isc HR department for December open vacation plan and list.

1) Please do note that all the names highlighted in green are the staff approved for open vacation, so if your name did not appear in green you are not eligle for a vacation.

2) Termination and contract employees, are marked in yellow color and it indicates staff status to be approved. Kindly return your response and also provide tentative date on or before COB 14th March 2023.

Please revert in writing, should you have further questions.

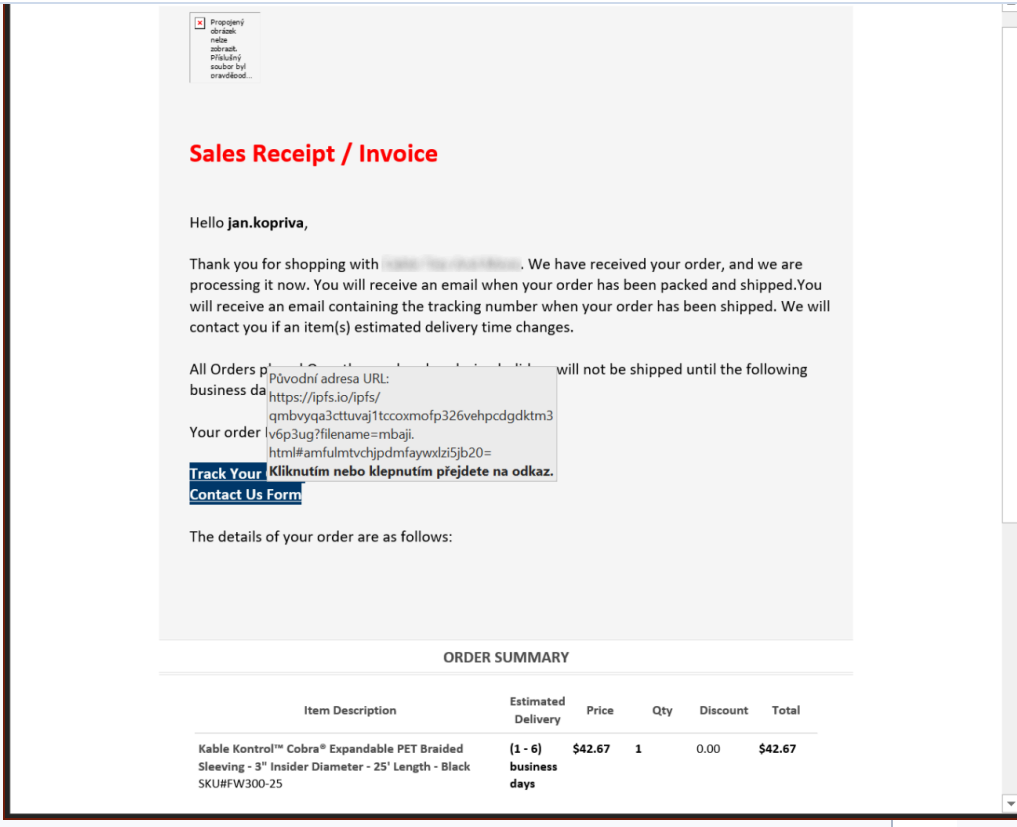
Thanks & Regards,

Director of Human Resources

Isc

Email : hr@isc.sans.edu

IMPORTANT - this e-mail and the information that it contains may be confidential, legally privileged and protected by law. Access by the intended recipient only is authorised. Any liability (in negligence or otherwise) arising from any third party acting, or refraining from acting, on any information contained in this e-mail is hereby excluded. If you are not the intended recipient, please notify the sender immediately and do not disclose the contents to any other person. The author also asserts the right to be identified as such and object to any misuse. Opinions expressed in this e mail are those of the individual and do not necessarily represent the opinions of the company.



Sales Receipt / Invoice

Hello **jan.kopriva**,

Thank you for shopping with . We have received your order, and we are processing it now. You will receive an email when your order has been packed and shipped.You will receive an email containing the tracking number when your order has been shipped. We will contact you if an item(s) estimated delivery time changes.

All Orders p will not be shipped until the following business da

Původní adresa URL: https://ipfs.io/ipfs/qmbvyqa3cttuvaj1tccoxmofp326vehpcdgdktm3v6p3ug?filename=mbaji.html#amfulmtvchjpdmfaywxlzi5jb20=
Kliknutím nebo klepnutím přejdete na odkaz.

Your order

Track Your

Contact Us Form

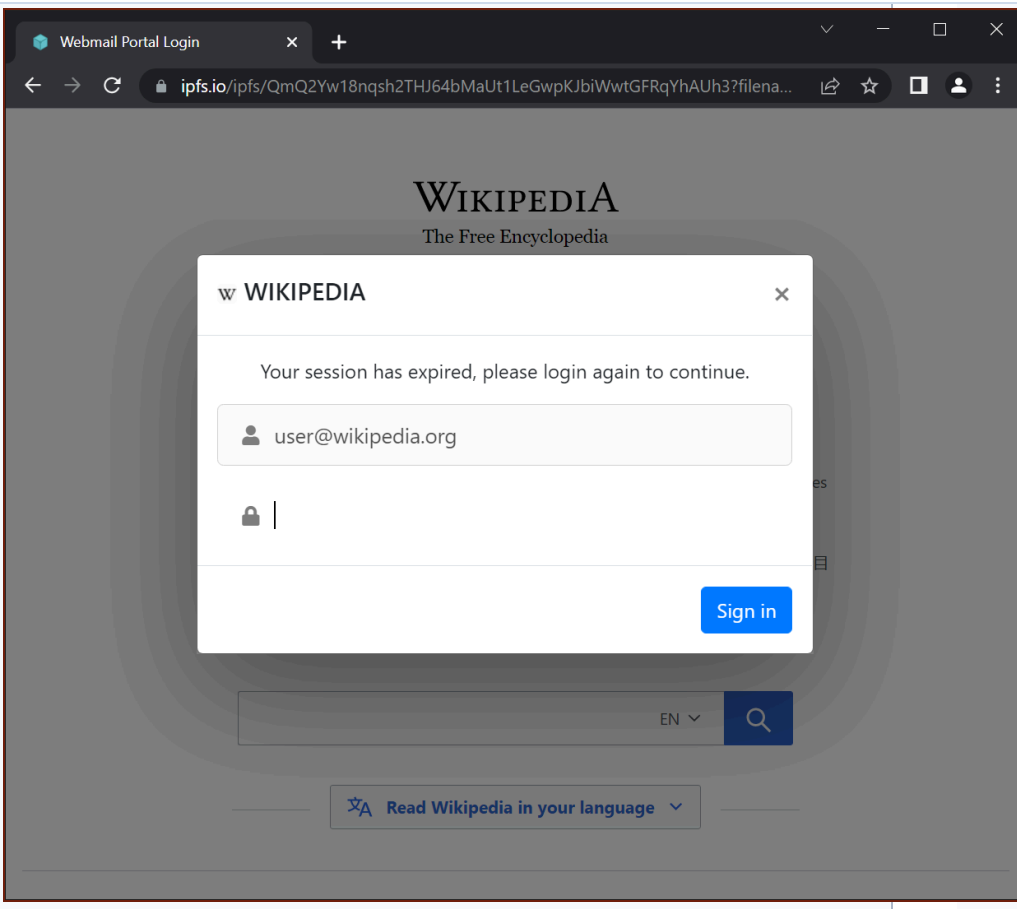
The details of your order are as follows:

ORDER SUMMARY

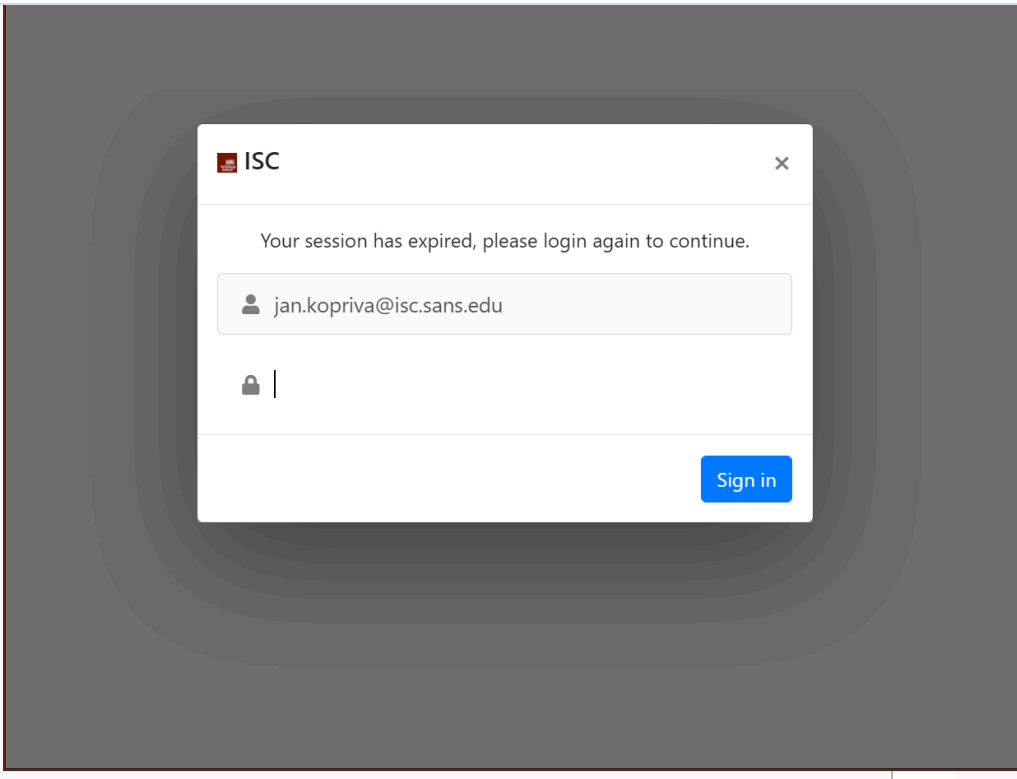
Item Description	Estimated Delivery	Price	Qty	Discount	Total
Kable Kontrol™ Cobra® Expandable PET Braided Sleeving - 3" Insider Diameter - 25' Length - Black SKU#FW300-25	(1 - 6) business days	$42.67	1	0.00	$42.67

...the HTML pages they linked to were very similar and all used the same clickjacking-related "login overlay over a legitimate website" trick.

This technique has been with us for a while now. It is based on the use of a HTML page, on which a fake login form is placed over an iframe, in which a legitimate website is loaded from a domain corresponding to the e-mail address of the recipient of the original phishing message. Since the e-mail address is (usually) passed to the phishing page in a parameter and the corresponding legitimate website is loaded dynamically, the result may look relatively believable, even though the fake login page was not tailor-made for a specific "target" individual or organization.



However, if the Content Security Policy and/or the X-Frame-Options HTTP headers are set, which is one of the standard defenses against clickjacking[2], the resulting login page is much less believable, as you may see in the following image...



Since clickjacking defenses have historically been used primarily to protect websites with sensitive functionalities and/or login forms, relevant security headers may not always be set for the “main website” of an organization.

However, as this phishing shows (and as do many others we’ve seen before), the lack of these headers on almost any website can potentially be a problem. Therefore, maybe the time has come to make CSP and other HTTP security headers the norm and not the exception. Although their use can sometimes be a little problematic, the corresponding issues can always be solved, and the simple use of few HTTP headers can make phishing attempts, such as the ones mentioned above, much less effective.

[2] https://owasp.org/www-community/attacks/Clickjacking

Jan Kopriva
@jk0pr
Nettles Consulting

Keywords: HTML HTTP Phishing

0 comment(s)

previous next

Comments

Login here to join the discussion.

Top of page

Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us

Slack Channel
Mastodon
Bluesky
X

Diary Archives