

Scammers are Exploiting Ukraine Donations

 mcafee.com/blogs/other-blogs/mcafee-labs/scammers-are-exploiting-ukraine-donations/

April 1, 2022



McAfee Labs

Apr 01, 2022

7 MIN READ

Authored by Vallabh Chole and Oliver Devane

Scammers are very quick at reacting to current events, so they can generate ill-gotten gains. It comes as no surprise that they exploited the current events in Ukraine, and when the Ukrainian Twitter account tweeted Bitcoin and Ethereum wallet addresses for donations we knew that scammers would use this as a lure for their victims.



Ukraine / Україна
@Ukraine



Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum and USDT.

BTC - 357a3S09CbsNfBBgFYACGvxxS6tMaDoa1P

ETH and USDT (ERC-20) -
0x165CD37b4C644C2921454429E7F9358d18A45e14

8:59 PM · Feb 26, 2022 · Twitter for iPhone

59.3K Retweets 13.7K Quote Tweets 216.6K Likes

This blog covers some of the malicious sites and emails McAfee has observed in the past few weeks.

Crypto wallet donation scams

A crypto donation scam occurs when perpetrators create phishing websites and emails that contain cryptocurrency wallets asking for donations. We have observed several new domains being created which perform this malicious activity, such as ukrainehelp[.]world and ukrainethereum[.]com.

Ukrainehelp[.]world

Below is a screenshot of Ukrainehelp[.]world, which is a phishing site asking for crypto donations for UNICEF. The website contains the BBC logo and several crypto wallet addresses.




While investigating this site, we observed that the Ethereum wallet used use was also associated with an older crypto scam site called eth-event20.com. The image below shows the current value of the crypto wallet which is worth \$114,000. Interestingly this wallet transfers all its coins to 0xc95eb2aa75260781627e7171c679a490e2240070 which in turn transfers to 0x45fb09468b17d14d2b9952bc9dcb39ee7359e64d. The final wallet currently has 313 ETH which is worth over \$850,000. This shows the large sums of money scammers can generate with phishing sites.

Address

USD 

This address has transacted 59 times on the Ethereum blockchain. It has received a total of 42.988967854029418013 ETH (\$115,050.08) and has sent a total of 42.896685955852454 ETH (\$114,803.11). The current value of this address is 0.000000000000000000 ETH (\$0.00).



Hash	0xb535c44555e001139c09dba74257cf54ddfb42d 
Nonce	36
Number of Transactions	59
Final Balance	0.00000000 ETH
Total Sent	42.896685955852454423 ETH
Total Received	42.988967854029418013 ETH
Total Fees	0.09228189817696359 ETH

Ukrainethereum[.]com

Ukrainethereum[.]com is another crypto scam site, but what makes this one interesting is the features it contains to gain the victim's confidence in trusting the website such as a fake chatbox and a fake donation verifier.

Home Donate Transactions Check your Donation

Take part in helping Ukraine during this unwanted war by Ethereum Donation!

During this unfortunate event we will try to help the Ukrainian citizens and give them a chance to recover from the war crisis. Be humane, let's show that we are more powerful when we are united.

Participate in Donation

ETH / USD +6.10%	BNB / USD +2.49%	XRP / USD +3.76%	XLM / USD 0%	DOGE / USD 0%	BTC / USD +0.120%
2 627.81 \$	380.8 \$	0.736 \$	0.176 \$	0.123 \$	38 918.34 \$

NEW DONATION EVENT FROM ETH

Donate and make Ukraine peaceful again


Follow the steps down below to participate in this donation

Hurry up and take part in this donation!

You can send ETH to the following address:

0x4E23u0FVFD365r7u784N62NC663036A79E796

Ukraine is waiting for your help.



Or scan the QR Code

297 675 ETH / 500 000

Make sure you donated

Donation is available for wallets that have not previously participated in this distribution

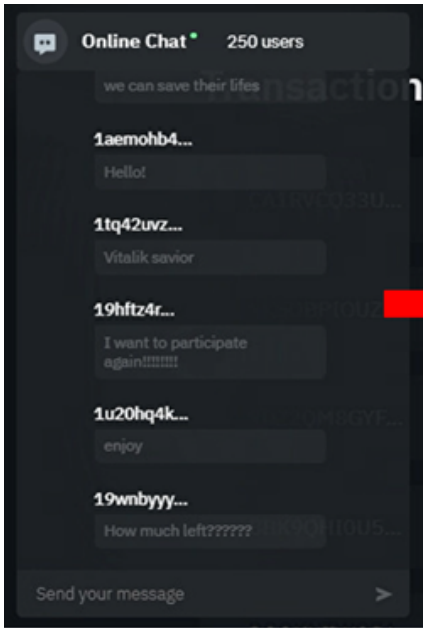
Online Chat* 2/18 users

Check

Fake Chat

Fake Donation Checker

Fake Chat



```

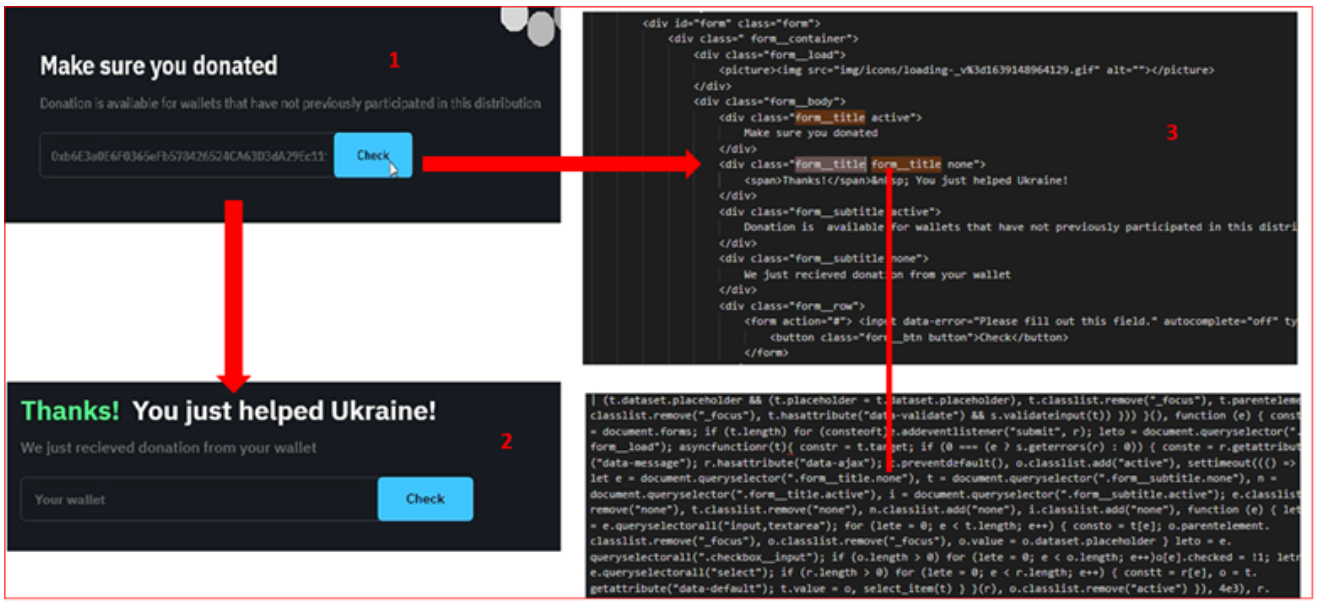
(" _error", e.parentelement.classList.remove("_error"), e.parentelement.querySelector(".form__error") && e.
parentelement.removeChild(e.parentelement.querySelector(".form__error"))); emailtest: e => /!^w*(\.-]?w*)@w+
[\.-]?w*(\.-]?w*(2,8))+$/ .test(e.value) ); $(function () { $("#chat-head").click(function () { $("#chat-body").
toggleclass("chat-active"), $("#chat").toggleclass("active") })); $(function () { $("#chat-close").click(
(function () { $("#chat-body").toggleclass("chat-active") })); letc = ["let'shelpukraine,
theydon'tdeservethis", "youguysaredoinggreatjob,onewordangels", "ukraine♥", "russiapleasestopthiswar",
"innocentarerying", "therearekids", "fuck", "veryniceguys", "ukrainejustdonated,greetingsfromusa!", "putindown",
"мижир", "let'ssaveukraine", "theyneedourhelp", "wecansavetheirlives", "omgongong", "ukraine..c3..",
"makeusproud", "thanksmates", "9.34eth", "cryptosabubble..", "justdonated", "staysafeukrainians", "++",
"russiadown!!", "vitalikweloveyou!!!", "2digitsforukraine", "youbetterbefastguy!", "vitalikneverdisappoints!!",
"enjoy", "willyoumakeanotherdonation???", "canidonatewithmatic?", "donationdonec3", "pimp", "ukraineneedsussss",
"vitaliksvlor", "godblessyou!", "prayforukraine", "kyivc3", "ghostofkyiv", "4.32eth", "ohhhherearesome$$$$$$",
"thankyouvitalikbuterin!.", "7.8eth", "ethtothemoon", "bigpumpiscoming", "thankyouforeverything.", "whaaaaaah???",
"3eth", "this is big deal nice vitalik!", "bigthanksfromukraine", "suka", "blyad!",
"let'splaydota2russians:d:d:d:d:", "этонизде", "ohyes!", "едать", "ethtothemoon", "wow", "русскисеукраиной",
"pumppp", "русскеубилиукраину", "canidonateevenmore?", "суважением", "rimca", "thanks!", "последняяшина",
"howisthispossible?", "helloeveryone!", "какже", "buterinisthebest", "howmuchleft?????", "supportukraine!",
"really?", "buterinistheking!", "elonthanksforstarlink", "justdonated2eth", "greatguys", "flex",
"iloveyouvitalik", "that'sgood!", "gotsome!", "heyyy", "mygod", "2eth?yeah", "howyoudoingguys?xd", "woooooow!!!",
"howcanicontactvitalik", "unbelievablecharity!", "donated7.27!!!!!!!!", "that'sgreatfull", "changedmymindoneth.
thankyou!", "5.34", "ethgoes1mil5", "thanksmuch!!!!", "iwanttoparticipateagain!!!!!!!!",
"ukrainawillriseagaininnn!!!!", "niceworksofar", "verygood.", "icantbelievit", "csgo3", "tellyourfriends!",
"ilovesimple", "that'sbeautiful!", "sovieunion", "toogood!", "eth4life", "iwillrememberthismomentforever!",
"thankgodinmonte", "thisissick!", "thisismagic", "justnice", "hieveryone", "restukrainians",
"iloveyouvitalikbuterin!!", "iblessyoueth!!", "cncw60", "thanksforlettingmeparticipate!", "should'vedespitedmore
...", "hello!", "привет", "украинаc3c3c3", "usaiswithukranc3", "ooooomgg!!!!!!!!!!!!!!!!!!!!!!", "спасибомир",
"thankgod.", "letsogod,letshelp", "eth$10ksoon", "kyivc3", "chillout", "2.4ethdonated", "goodluckeveryone,
hopeyoustay safe!", "sohappy!", "omg!!!!!!", "thanks", "whoelseifnotvitalikcouldhelpus", "vitalikbuterin!!", "35.
3874eth", "yeah", "imverythankful", "newethathcoming", "perfect", "weloveyouvitalik", "hi",
"iwishihadmoreethtosend", "+2.1", "thatsforreal", "itisactual", "awesome", "+7.4288", "ethgoes100k", "ethrocket",
"letu = document.querySelector(".chat__iduser"); function(e, t) { returnmath.floor(math.random() * (t - e + 1)) +
e } letm = document.getElementById("chat-body"), h = (setinterval(() => { letc = "1" + function (e) { for (var t =
"", o = "abcdefghijklmnopqrstuvwxyz0123456789", r = o.length, n = 0; n < e; n++) t += o.charAt(math.floor(math.
random() * r)); return t })(7) + "...", t = c[math.floor(math.random() * c.length)], o = document.createElement
("div", r = 0(1, 20); o.className = "mess", o.setAttribute("style", "--bg:url(..../img/avatar/avatar + r + ".png)",
console.log("--bg:url(..../img/avatar/avatar + r + ".png)", o.innerHTML = "<divclass='msg'><class='nickname'>$
(e)</p><class='msg-text'>${t}</p></div>", m.appendChild(o), $("#chat-body").scrollTop($("#chat-body")[0].
scrollheight, o.innerHTML = d(220, 300) ), 4e3), document.querySelector(".chat_btn"), p = document.
querySelector(".chat__input"); h && h.addEventListener("click", (function () { if (p.value.length > 0) { letc =
document.createElement("div"); e.className = "messcolor"; const = math.floor(16777215 * math.random()).tostrin
g(16); e.setAttribute("style", "--color:#" + t), e.innerHTML = "<divclass='msg'><class='nickname'>you<
p><class='msg-text'>${p.value}</p></div>", m.appendChild(e), $("#chat-body").scrollTop($("#chat-body")[0].
scrollheight, p.value = "" })); vars, f; window.element && element.prototype.closest && (element.prototype.
closest = function (s) { var t = (this document || this).querySelector(s); if (t) do { for

```

The image above shows the chatbox on the left-hand side which displays several messages. At first glance, it would appear as if other users are on the website and talking, but when you reload the site it shows the same messages. This is due to the chat messages being displayed from a list that is used to populate the website with JavaScript code as shown on the right-hand side.

Fake Donation Verifier

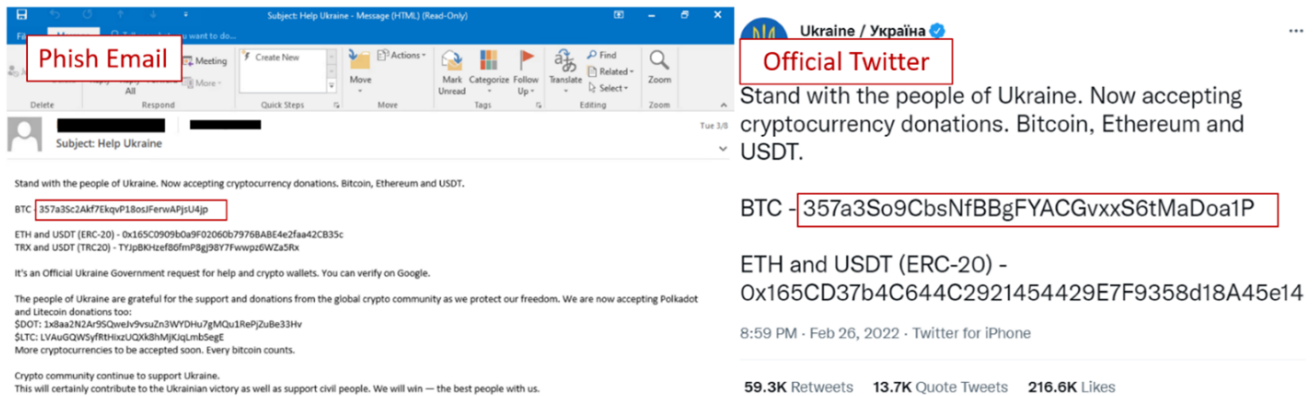
The site contains a donation checker so the victim can see if their donation was received, as shown below.



1. The first image on left shows the verification box for donation to check if it is completed or not
2. Upon clicking 'Check' the victim is shown a message to say the donation was received.
3. What occurs, is upon clicking 'Check' the JavaScript code changes the website code so that it displays the 'Thanks!' message, and no actual check is performed.

Phishing Email

The following image shows one of the examples of phish emails we have observed.



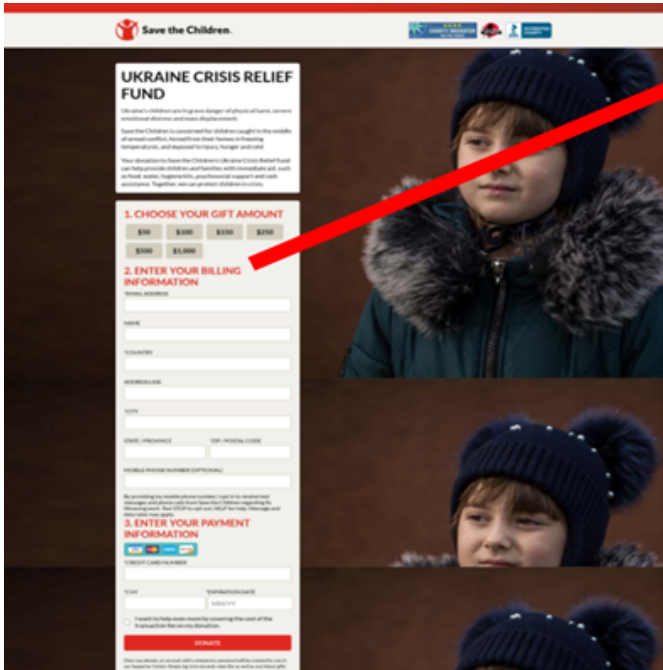
The email is not addressed to anyone specifically as they are mass-mailed to multiple email addresses. The wallet IDs in the email are not associated with the official Ukraine Twitter and are owned by scammers. As you can see in the image above, they are similar as the first 3 characters are the same. This could lead to some users believing it is legitimate. Therefore, it's important to check that the wallet address is identical.

Credit Card Information Stealer

This is the most common type of phishing website. The goal of these sites it entices the victim into entering their credit card and personally identifiable information (PII) data by making them believe that the site being visited is official. This section contains details on one such website we have found using Ukraine donations as a lure.

Razonforukrain[.]com

The image below shows the phishing site. The website was used to save the children's NGO links and images, which made it appear more genuine. You can see that is it asking the victim to enter their credit card and billing information.



```

</div>
<form action="telegram.php" method="post">
  <div class="input_box">
    <input type="text" name="email" required="">
  </div>
  <div class="input_box">
    <input type="text" name="name">
  </div>
  <div class="input_box">
    <input type="text" name="country" required="">
  </div>
  <div class="input_box">
    <input type="text" name="address" required="">
  </div>
  <div class="input_box">
    <input type="text" name="city">
  </div>
  <div class="input_box_double">
    <input type="text" name="state">
  </div>
  <div class="input_cont">
    <input type="text" name="zip">
  </div>
  <div class="input_box">
    <input type="text" class="cvv" name="phone">
  </div>
  <div class="input_box">
    <input type="text" class="cvv" name="phone">
  </div>
  <div class="input_box">
    <input type="text" class="card" name="card" required="">
  </div>
  <div class="input_box_double">
    <input type="text" class="cvv" maxlength="3" name="cvv" required="">
  </div>
  <div class="input_cont">
    <input type="text" class="exp" placeholder="MM/YY" name="exp" required="">
  </div>
</form>

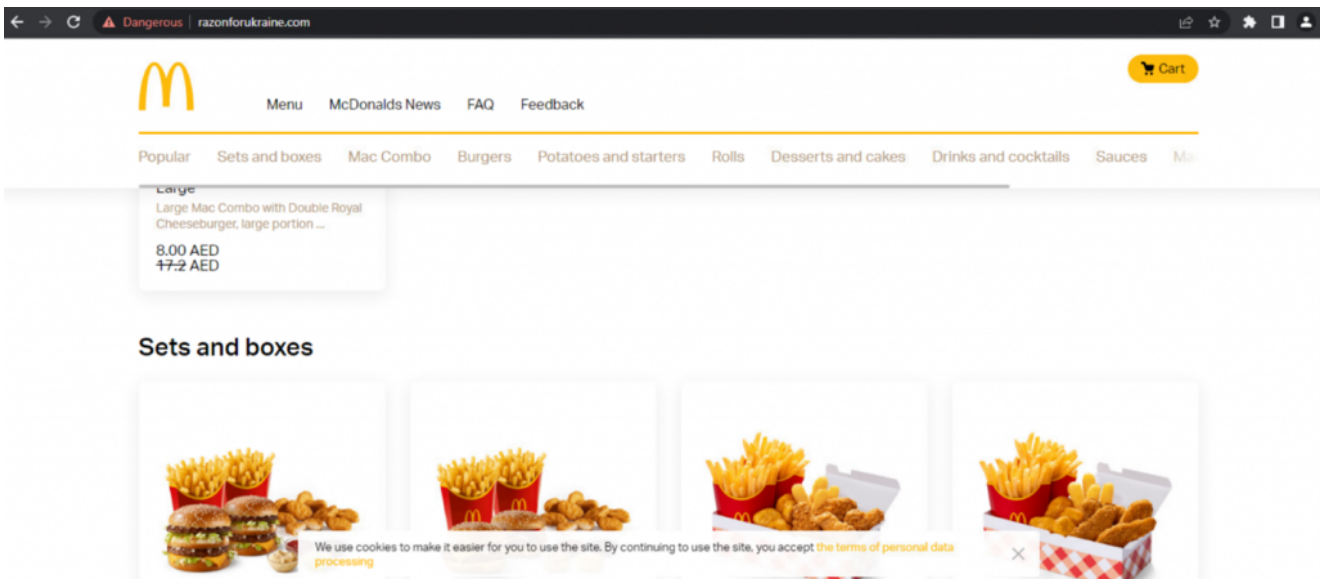



</div>
<div class="input_box">
  <input type="text" class="card" name="card" required="">
</div>
<div class="input_box_double">
  <input type="text" class="cvv" maxlength="3" name="cvv" required="">
</div>
<div class="input_cont">
  <input type="text" class="exp" placeholder="MM/YY" name="exp" required="">
</div>
</div>

```

Once the data is entered, and the victim clicks on 'Donate', the information will be submitted via the form and will be sent to scammers so they can then use or sell the information.

We observed that a few days after the website was created, the scammers change the site code so that it became a McDonald's phishing site targeting the Arab Emirates. This was a surprising change in tactics.



The heatmap below shows the detections McAfee has observed around the world for the malicious sites mentioned in this blog.



Conclusion

How to identify a phishing email?

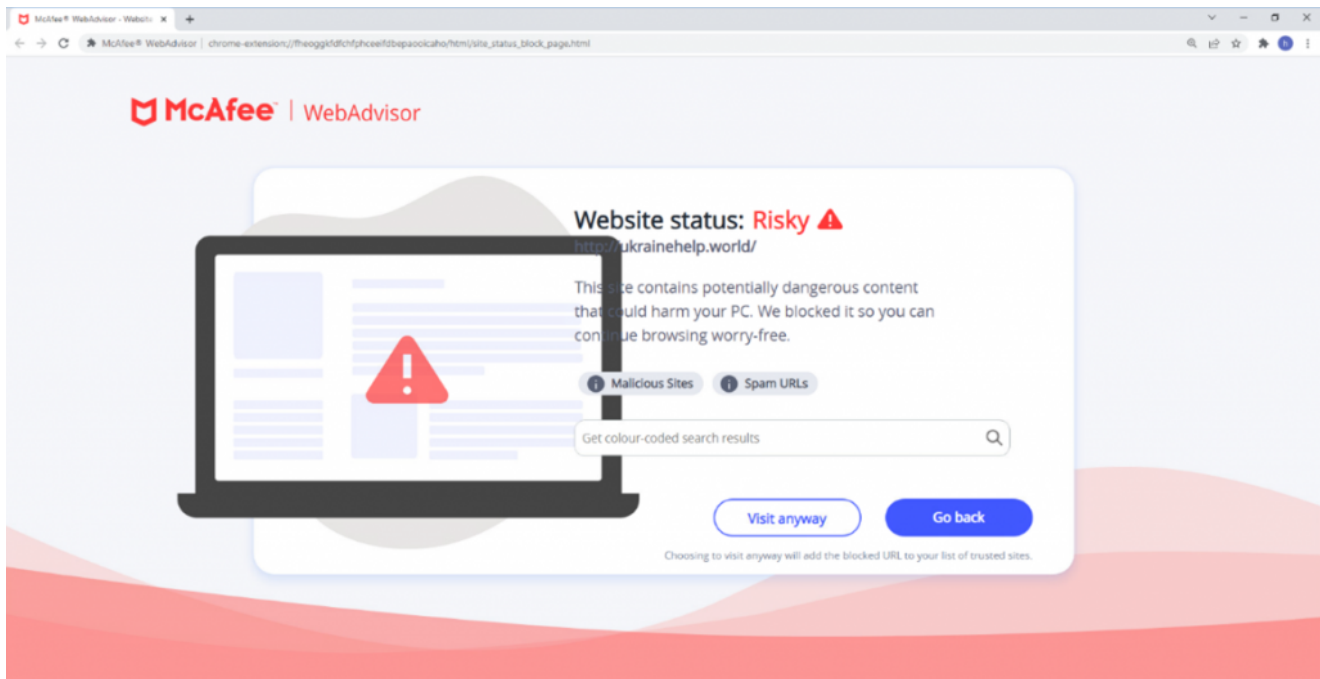
- Look for the domain from where you received mail, attackers masquerade it.
- Use McAfee Web Advisor as this prevents you from accessing malicious sites
- If McAfee Web Advisor is not used, links can be manually checked at <https://trustedsource.org/>.
- Perform a Web Search of any crypto wallet addresses. If the search returns no or a low number of hits it is likely fraudulent.
- Check for poor grammar and suspicious logos
- For more detailed advice please visit McAfee's How to recognize and protect yourself from [phishing page](#)

How to identify phishing websites?

- Use McAfee Web Advisor as this prevents you from accessing malicious sites
- Look at the URL of the website which you are visiting and make sure it is correct. Look for alterations such as login-paypal.com instead of login.paypal.com
- If you are unsure that the website is legitimate. Perform a Web search of the URL. You will find many results if they are genuine. If the search returns no or a low number of hits it is likely fraudulent
- Hyperlinks and site addresses that do not match the sender – Hover your mouse over the hyperlink or call-to-action button in the email. Is the address shortened or is it different from what you would expect from the sender? It may be a spoofed address from the
- Verify if the URL and Title of the page match. Such as the website, [razonforukraine\[.\]com](#) with a title reading “McDonald’s Delivery”

For general cyber scam, education click [here](#)

McAfee customers are protected against the malicious sites detailed in this blog as they are blocked with McAfee Web Advisor



Type	Value	Product	Detected
URL – Phishing Sites	ukrainehelp[.]world	McAfee WebAdvisor	Blocked
URL – Phishing Sites	ukrainethereum[.]com	McAfee WebAdvisor	Blocked
URL – Phishing Sites	unitedhelpukraine[.]kiev[.]ua/	McAfee WebAdvisor	Blocked
URL – Phishing Sites	donationukraine[.]io/donate	McAfee WebAdvisor	Blocked
URL – Phishing Sites	help-ukraine-campaign[.]com/shop	McAfee WebAdvisor	Blocked
URL – Phishing Sites	ukrainebitcoin[.]online/	McAfee WebAdvisor	Blocked
URL – Phishing Sites	ukrainedonation[.]org/donate	McAfee WebAdvisor	Blocked
URL – Phishing Sites	ukrainewar[.]support	McAfee WebAdvisor	Blocked

URL – Phishing Sites	sendhelptoukraine[.]com	McAfee WebAdvisor	Blocked
URL – Phishing Sites	worldsupportukraine[.]com	McAfee WebAdvisor	Blocked
URL – Phishing Sites	paytoukraine[.]space	McAfee WebAdvisor	Blocked
URL – Phishing Sites	razonforukraine[.]com	McAfee WebAdvisor	Blocked

McAfee Labs Threat Research Team

McAfee Labs is one of the leading sources for threat research, threat intelligence, and cybersecurity thought leadership. See our blog posts below for more information.

More from McAfee Labs

Crypto Scammers Exploit: Elon Musk Speaks on Cryptocurrency

By Oliver Devane Update: In the past 24 hours (from time of publication) McAfee has identified 15...

May 05, 2022 | 4 MIN READ

Instagram Credentials Stealer: Disguised as Mod App

Authored by Dexter Shin McAfee’s Mobile Research Team introduced a new Android malware targeting Instagram users who...

May 03, 2022 | 4 MIN READ

Instagram Credentials Stealers: Free Followers or Free Likes

Authored by Dexter Shin Instagram has become a platform with over a billion monthly active users. Many...

May 03, 2022 | 6 MIN READ



Imposter Netflix Chrome Extension Dupes 100k Users

Authored by Oliver Devane, Vallabh Chole, and Aayush Tyagi McAfee has recently observed several malicious Chrome Extensions...

Mar 10, 2022 | 8 MIN READ



Why Am I Getting All These Notifications on my Phone?

Authored by Oliver Devane and Vallabh Chole Notifications on Chrome and Edge, both desktop browsers, are commonplace,...

Feb 25, 2022 | 5 MIN READ



Emotet's Uncommon Approach of Masking IP Addresses

In a recent campaign of Emotet, McAfee Researchers observed a change in techniques. The Emotet maldoc was...

Feb 04, 2022 | 4 MIN READ



HANCITOR DOC drops via CLIPBOARD

Hancitor, a loader that provides Malware as a Service, has been observed distributing malware such as FickerStealer,...

Dec 13, 2021 | 6 MIN READ



'Tis the Season for Scams

'Tis the Season for Scams

Nov 29, 2021 | 18 MIN READ



The Newest Malicious Actor: "Squirrelwaffle" Malicious Doc.

Authored By Kiran Raj Due to their widespread use, Office Documents are commonly used by Malicious actors...

Nov 10, 2021 | 4 MIN READ



Social Network Account Stealers Hidden in Android Gaming Hacking Tool

Authored by: Wenfeng Yu McAfee Mobile Research team recently discovered a new piece of malware that specifically...

Oct 19, 2021 | 6 MIN READ



Malicious PowerPoint Documents on the Rise

Authored by Anuradha M McAfee Labs have observed a new phishing campaign that utilizes macro capabilities available...

Sep 21, 2021 | 6 MIN READ



Android malware distributed in Mexico uses Covid-19 to steal financial credentials

Authored by Fernando Ruiz McAfee Mobile Malware Research Team has identified malware targeting Mexico. It poses as a security banking tool or...

Sep 13, 2021 | 7 MIN READ

