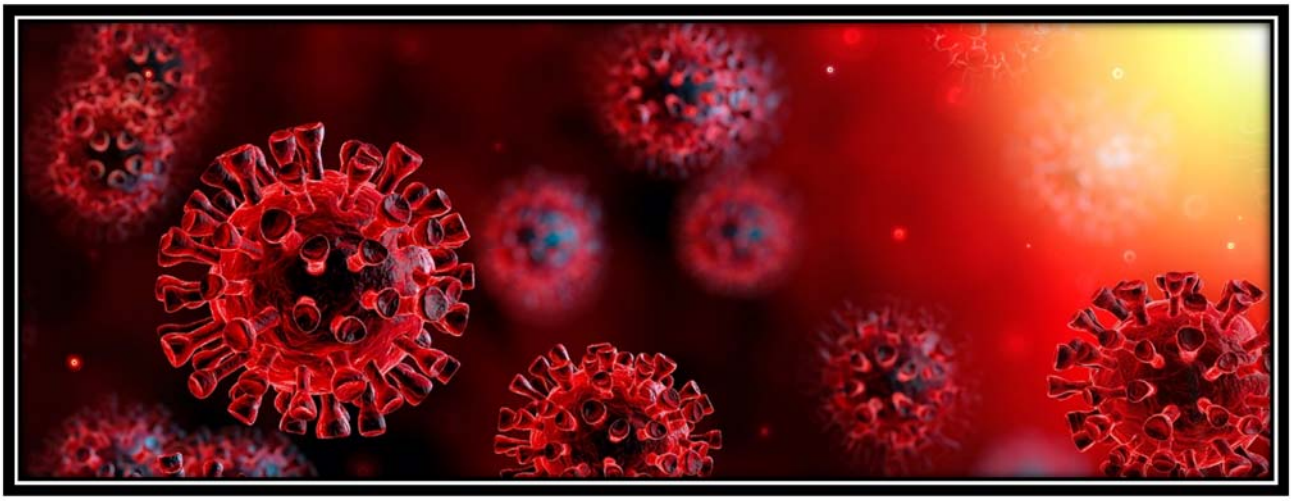
الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

National Agency for Network Services

فيروس كورونا والتصيّد الإلكتروني

انتحال قراصنة الإنترنت هويّة مركز السيطرة على الأمراض CDC ومنظّمة الصحة العالمية WHO



إعداد: م. سُليمه مسلم كنينه

مركز أمن المعلومات

التصيّد الإلكتروني أو التصيّد الاحتيالي: هو هجوم إلكتروني للحصول على معلومات حساسة مثل حسابات المستخدمين وكلمات المرور الخاصة بها، ويعتمد على أساليب التنكر ككيان جدير بالثقة (موقع إلكتروني-تطبيق-البريد الإلكتروني) لخداع المستخدمين.

مع استمرار انتشار فيروس كورونا COVID-19، نشهد زيادة في نشاط قراصنة الإنترنت لانتحال هويّة منظمات الصحة العامّة والوكالات الحكومية لخداع الضحايا.

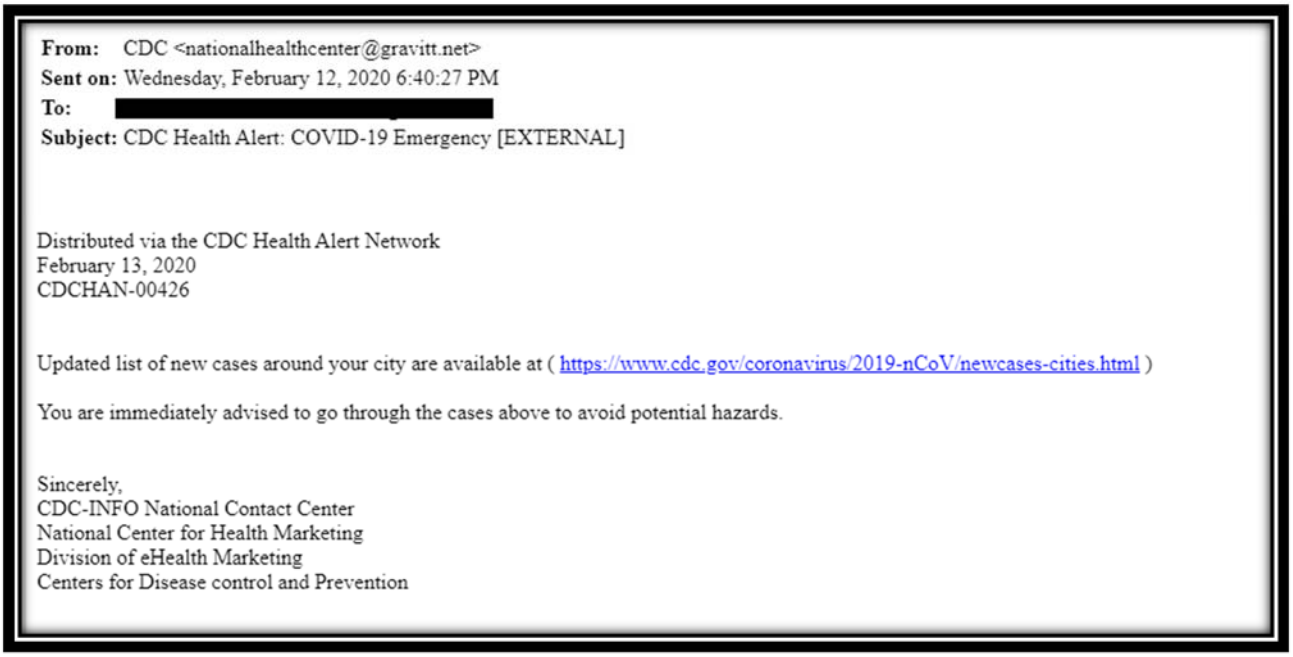
الأمثلة الأربعة أدناه عبارة عن انتحال هويّة مركز السيطرة على الأمراض والوقاية منها (CDC) ومنظمة الصحة العالمية (WHO) ونلاحظ فيها أن المهاجم يقوم بإنشاء مواقع مزيفة وإرسال الروابط المزيفة إلى عدد كبير من مستخدمي الشبكة العنكبوتية وبطرق عديدة مثل رسائل البريد الإلكتروني:

مثال(1):

احتيال لسرقة بيانات الاعتماد الخاصة ببريد الويب

في هذا المثال، يستخدم المهاجم خدمة **SendGrid** (وهي خدمة تسويق عبر البريد الإلكتروني) لتوزيع عنوان البريد الإلكتروني المزيّف لمركز الصحة الوطني، يدّعي الرابط الموجود في الرسالة أنه يوفر قائمة محدّثة للحالات الجديدة، ولكنّه في الواقع يقود الضحيّة إلى تصيّد البريد الإلكتروني بنيّة سرقة بيانات تسجيل الدخول لحساب الضحية.

المرسل (المُهاجم): nationalhealthcenter@gravitt.net



From: CDC <nationalhealthcenter@gravitt.net>
Sent on: Wednesday, February 12, 2020 6:40:27 PM
To: [redacted]
Subject: CDC Health Alert: COVID-19 Emergency [EXTERNAL]

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

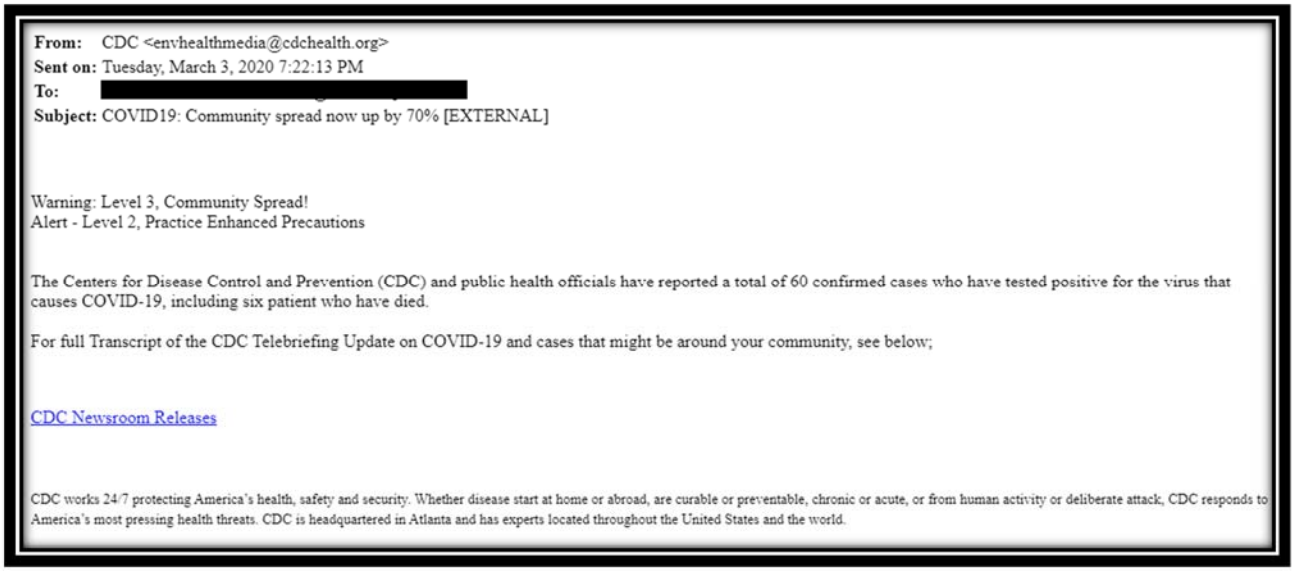
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

مثال(2):

في المثال الثاني، قام المهاجم بإنشاء نطاق مزيّف وذلك للخداع والاحتيال واستضاف الموقع المعد للتصيّد الإلكتروني عليه أيضًا وهو:http://url4510.cdchealth.org

على غرار ما ورد أعلاه، يتم استخدام خدمة SendGrid مع العنوان الفعلي الذي ينشأ من خادم Amazon AWS.

النطاق المزيف: CDCHEALTH.ORG



From: CDC <envhealthmedia@cdchealth.org>
Sent on: Tuesday, March 3, 2020 7:22:13 PM
To: [redacted]
Subject: COVID19: Community spread now up by 70% [EXTERNAL]

Warning: Level 3, Community Spread!
Alert - Level 2, Practice Enhanced Precautions

The Centers for Disease Control and Prevention (CDC) and public health officials have reported a total of 60 confirmed cases who have tested positive for the virus that causes COVID-19, including six patient who have died.

For full Transcript of the CDC Telebriefing Update on COVID-19 and cases that might be around your community, see below;

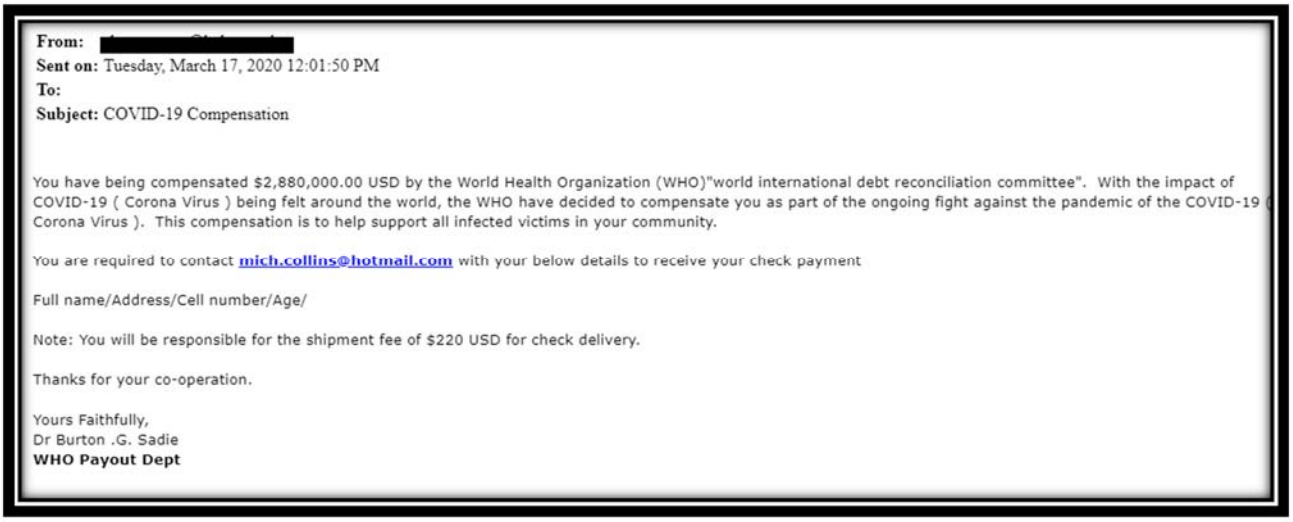
CDC Newsroom Releases

CDC works 24/7 protecting America's health, safety and security. Whether disease start at home or abroad, are curable or preventable, chronic or acute, or from human activity or deliberate attack, CDC responds to America's most pressing health threats. CDC is headquartered in Atlanta and has experts located throughout the United States and the world.

مثال(3):

احتيال الدفع

يقدّم المهاجم وعد بالدفع للضحية كجزء من التعويض عن فيروس كورونا.
تم اختراق عنوان المرسل، ولهذا السبب يوجّه المجرم الإلكتروني الضحيّة إلى الرد على البريد الإلكتروني التالي mich.collins@hotmail.com من أجل الحصول على تعويض.
ومن بين العلامات التحذيريّة في هذه الرسالة هي الإيحاء للضحية بأنه من أجل أن تحصل على دفعتك، يجب عليك أولاً دفع مبلغ 220 دولار.



From: [redacted]
Sent on: Tuesday, March 17, 2020 12:01:50 PM
To:
Subject: COVID-19 Compensation

You have being compensated $2,880,000.00 USD by the World Health Organization (WHO)"world international debt reconciliation committee". With the impact of COVID-19 (Corona Virus) being felt around the world, the WHO have decided to compensate you as part of the ongoing fight against the pandemic of the COVID-19 (Corona Virus). This compensation is to help support all infected victims in your community.

You are required to contact **mich.collins@hotmail.com** with your below details to receive your check payment

Full name/Address/Cell number/Age/

Note: You will be responsible for the shipment fee of $220 USD for check delivery.

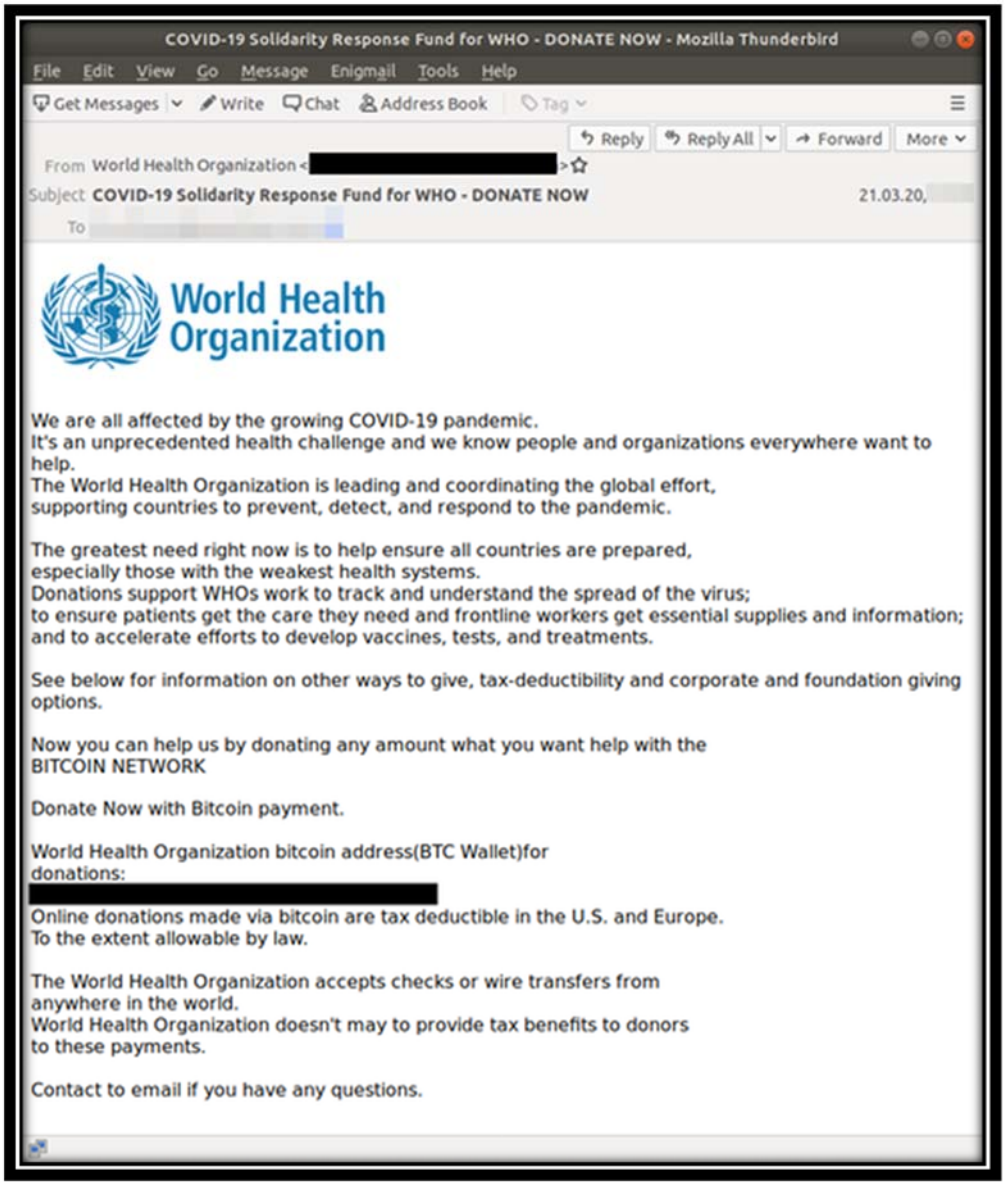
Thanks for your co-operation.

Yours Faithfully,
Dr Burton .G. Sadie
WHO Payout Dept

مثال (4):

احتيال التبرّع

يستخدم المهاجم عنوان بريد إلكتروني مزيّف لمنظمة الصحة العالمية في عملية احتيال للتبرّع.
حيث يطلب المهاجم من الضحية تحويل العملات الرقمية المشفّرة عبر محفظة بيتكوين.
إذا تم تنفيذه، فلن تكون هناك فرصة كبيرة لعكس المعاملة.



وطالما هذا الوباء موجود، فيمكن لقراصنة الإنترنت الاستفادة من الإحصائيات المتغيرة والبيانات الجديدة واستغلال حاجة الجمهور لهذه المعلومات ورغبة البعض بالمساعدة عن طريق الاحتيال عليهم بطرق شتى، ولذلك ننصح بالحذر والانتباه وعدم الاستجابة لأي من هذه الرسائل أو الدعوات مهما كان مصدرها، واستقاء المعلومات من المصادر الحكومية السورية الرسمية والتي لا تستخدم رسائل البريد الإلكتروني للتواصل مع الجمهور بطبيعة الحال.

ونأمل عند تلقي أي رسائل بريد إلكتروني تتضمن روابط مشبوهة عبر أي وسيلة تواصل إلكتروني ومشابهة للأمثلة التي ذكرناها أعلاه إعلام مركز أمن المعلومات في الهيئة الوطنية لخدمات الشبكة عبر البريد الإلكتروني infosec@nans.gov.sy لنقوم بتحليلها والتحذير منها إن تضمنت أي نوع من الهجمات الإلكترونية لتعم الفائدة على الجميع.

مع تمنياتنا لكم بدوام الصحة والسلامة