



**Right Click  
Solutions LLC**

small business computer consulting



**CYBERSECURITY  
AWARENESS  
MONTH**

**DO YOUR PART.  
#BECYBERSMART.**

**Cyber Security and the Pandemic –  
20 Seconds to Better Email Hygiene**





## Three examples of COVID-19 PHISHING EMAILS

**Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

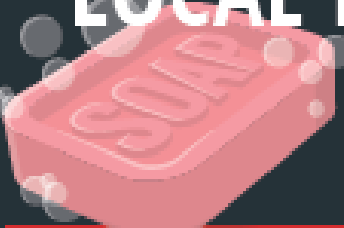
- Divulge private information - passwords, emails, personal data, documents, money
- Engage you in correspondence to gain trust
- Link to download malware or link to website for credential harvesting or malware
- Attachment that contains malware - ransomware, spyware, viruses, worms, Trojan horses, rogue software, adware and scareware
- Malware is software designed to cause damage to a computer, server, client, or network



## Three examples of COVID-19 PHISHING EMAILS Spreading Fear and Panic of Increased Local Infections

BEWARE: COVID-19 PHISHING EMAILS

# SPREADING FEAR AND PANIC OF INCREASED LOCAL INFECTIONS




Avoid COVID-19 phishing scams by practicing good email hygiene. The CDC recommends you take at least 20 seconds to wash your hands to avoid germs. We recommend you take at least 20 seconds to review each email to avoid falling victim to a phishing scam.



# Three examples of COVID-19 PHISHING EMAILS Spreading Fear and Panic of Increased Local Infections

## 2019-nCoV: Coronavirus outbreak in your city (Emergency)

 **CDC-INFO** <cdcchan-00813@cdc.gov.org>  
Tue 2/4/2020 8:33 AM  
To: John Smith

Distributed via the CDC Health Alert Network  
February 4, 2020  
CDCHAN-00813


Dear Sir/Madam,

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

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



**FAKE E-MAIL ADDRESS**


**TOO GENERIC**

**URGENCY**


**POOR GRAMMAR**

**LEGEND**

- FAKE E-MAIL ADDRESS
- TOO GENERIC
- BAD LINKS
- URGENCY
- SYNTAX & GRAMMATICAL ERRORS



**CHECK BEFORE YOU CLICK!**  
Hover your cursor over the link to preview the link URL. BEWARE of links that direct you to a login page.



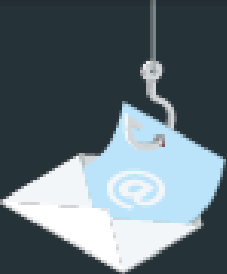

The fake web page use in the coronavirus phishing campaign looks like an Outlook login window



## Three examples of COVID-19 PHISHING EMAILS Exploiting Confused & Stressed Employees

**BEWARE: COVID-19 PHISHING EMAILS**

# EXPLOITING CONFUSED & STRESSED EMPLOYEES



Cyber criminals are exploiting headlines and global panic around the COVID-19 pandemic. Exercise extreme caution with any emails containing a COVID-19-related subject line, attachment, or hyperlinks. Be wary of social media pleas, texts, or calls related to COVID-19.

# Three examples of COVID-19 PHISHING EMAILS

## Exploiting Confused & Stressed Employees

### Policy Update: Communicable Diseases

Human Resources <hr@[company\_domain]> **FAKE E-MAIL ADDRESS**  
 Wed 3/18/2020 6:04 AM  
 To: John Smith

All, **TOO GENERIC**

Due to the coronavirus outbreak, [company\_name] is actively taking safety precautions by instituting a [Communicable Disease Management Policy](#). This policy is part of our organizational preparedness and we require all employees to read and **acknowledge the policy before** **[[current\_date\_1]]**. **URGENCY**

If you have any questions or concerns regarding the policy, please contact [company\_name] Human Resources.

Regards,  
Human Resources

**CHECK FOR FRAUDULENT LINKS**

**URGENT**  
Make sure company details are correct but also standard verbiage for your organization.

**LEGEND**

- FAKE E-MAIL ADDRESS
- TOO GENERIC
- BAD LINKS
- URGENCY





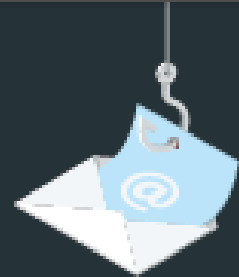
## Three examples of COVID-19 PHISHING EMAILS Safety Measures Deliver Malware Instead

BEWARE: COVID-19 PHISHING EMAILS

# SAFETY MEASURES DELIVER MALWARE INSTEAD



Cyber criminals are exploiting headlines and global panic around the COVID-19 pandemic. Exercise extreme caution with any emails containing a COVID-19-related subject line, attachment, or hyperlinks. Be wary of social media pleas, texts, or calls related to COVID-19.






# Three examples of COVID-19 PHISHING EMAILS

## Safety Measures Deliver Malware Instead

### Singapore Specialist : Corona Virus Safety Measures


**Hsing, Sheng** <sheng.hsing@who-pc.com>  
 Tue 1/28/2020 12:19 PM  
 To: John Smith

FAKE E-MAIL ADDRESS

Dear Sir, TOO GENERIC

Go through the attached document on safety measures regarding the spreading of corona virus.  
URGENCY


Use the link below to download

[Safety-Measures.pdf](#) CHECK FOR FRAUDLENT LINKS

POOR GRAMMAR

Symptoms Common symptoms include fever, cough, shortness of breath, and breathig difficulties. I


Regards,  
 Dr. Sheng Hsing  
 Specialist wuhan-virus-advisory



**UNUSUAL SENDER OR ACTION**  
 How often would you get a email directly from a doctor to your work email?

**LEGEND**

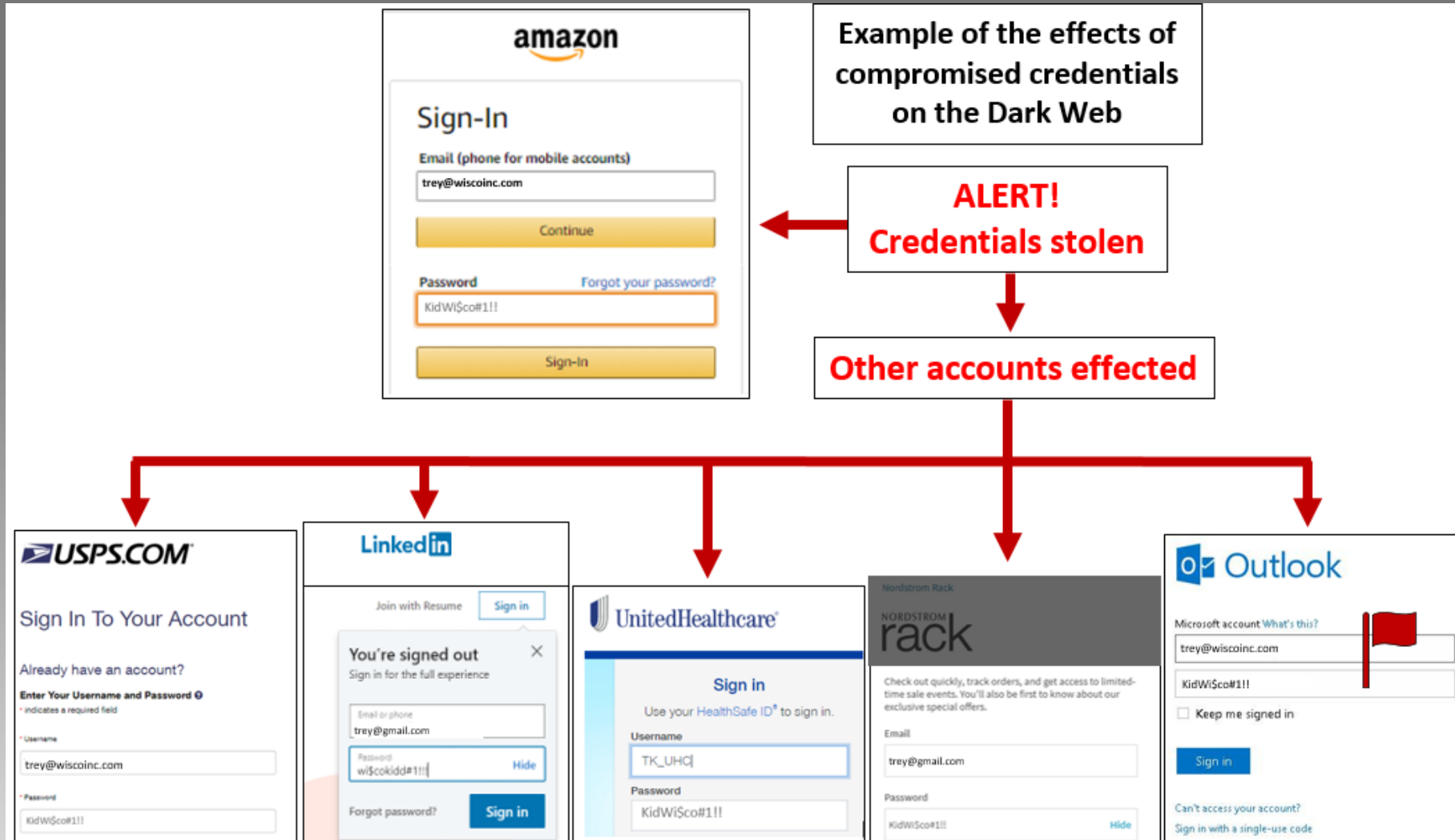
- FAKE E-MAIL ADDRESS
- TOO GENERIC
- BAD LINKS
- URGENCY
- SYNTAX & GRAMATICAL ERRORS







# What Can Happen if your Credentials are Compromised?





# Your Best Defense: Be Educated and Practice Good Email Hygiene

## 20 SECONDS TO BETTER EMAIL HYGIENE



**1**

### **WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS**

Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."

**2**

### **EXAMINE THE ENTIRE FROM EMAIL ADDRESS**

The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.

**3**

### **LOOK FOR URGENCY OR DEMANDING ACTIONS**

"You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

**4**

### **CAREFULLY CHECK ALL LINKS**

Mouse over the link and see if the destination matches where the email implies you will be taken.

**5**

### **NOTICE MISPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING**

This might be a deliberate attempt to try to bypass spam filters.

**6**

### **CHECK FOR SECURE WEBSITES**

Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

**7**

### **DON'T CLICK ON ATTACHMENTS RIGHT AWAY**

Attachments containing viruses might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised."



## Your Best Defense: Be Educated and Practice Good Email Hygiene

Worried if your email or domain has been compromised?

We can run a Dark Web ID scan on your email address or domain to determine if your credentials are on the Dark Web.

For more information about our partner ID Agent and their Dark Web ID product, or any of the products and services we offer, contact us at **team@rcsllc.net!**



27 Radio Circle Drive, Suite 104 · Mount Kisco, NY 10549 · p 914-242-3212 · [www.RCSLLC.net](http://www.RCSLLC.net)