# PREVENTING PHISHING ATTACKS

*"Are you safe yet?"*

## THE TEAM

From left to right: Coleman, Uialii; Andrews, Aleimah; Tabujara, MaiAngel; Hooks, Courtney; Hsu, Jocelyn; Addis, Isaac.

## HOSPITALS IN DANGER

By Jocelyn H.

The online security of computer usage is now being compromised by malicious attachments and links in emails. Hospitals, especially in Los Angeles County, have been hacked because they have patient information. With 129 hospitals helping a population of more than ten million people, Los Angeles County is the perfect target for hackers. If a LA hospital computer system is shut down, the hospital would be forced to pay the ransom money since it relies on the technology for their patient's record. Although a designated group of staff have been trained to identify suspicious emails, criminals nowadays make convincing campaigns. Unfortunately, these are difficult to identify with a quick glance. Current technology warns people about attachments or links in every email, but there is no software that scans for these potentially dangerous messages.

BitEruptor Technologies, a new company founded on March 8, 2016, is designed to tackle these phishing scams. Its mission is to prevent hackers from gaining access to private information from hospitals. BitEruptor has designed software, called BitEruption, designated to scan for harmful email attachments to warn hospital employees about potential viruses that could shut down the entire computer system in the hospital. With the program downloaded, phishing scams are no longer a problem that hospital staff need to worry about.


BitEruptor works towards eliminating cyber scams

Photo courtesy of BitEruptor

## CYBER ISSUES THAT HOSPITALS FACE

### Hollywood Presbyterian Medical Center Phishing Scam

By MaiAngel T.

The Hollywood Presbyterian Medical Center is located in Los Angeles, CA. This medical center has had an attack in which their computers' security system lacked reliability thus leading hackers to be able to, easily, get into their system. Their computers and the information in it were held "hostage" through a computer network's data developed by hackers. The Hollywood Presbyterian Medical Center ended up paying hackers a ransom of 40 bitcoins, equal to approximately $17,000 dollars. Workers at this medical center/hospital stated, "it was the easiest way out of the problem." Clearly, they did not have any type of software/program to protect them from situations like this.

### How Hospitals are Hacked

By Courtney H.

Cyber attacks usually occur to steal a person's identity, hack into their accounts, trick them into revealing their personal information, or infect their devices with malware. Cyber attacks are mostly committed in small groups or by an individual. It is very hard to track down these threats because they act anonymously when it comes to global positioning, names, and identities. Some attack techniques that attackers uses are Social Engineering, and Fast Flux. Phishing can be identified as a Social Engineering or a Fast Flux attack and is used to steal information from banks, small businesses, and especially hospitals. LA hospitals are the most vulnerable to attacks because their infrastructure is so large and vital that any amount of information lost could majorly damage that hospital. Hackers are able to hack hospitals by sending emails with links, which hospital staff can click on, and gain access to patients' information.

## CURRENT SOLUTION USED BY DOCTORS WITHOUT BORDERS


"Surfing the Web"

Photo courtesy of Doctors Without Borders

By Aleimah A.

The staff of Doctors Without Borders has dedicated their time and efforts to provide medical attention for people in developing countries and disaster stricken areas. This is why their staff typically do not have access to the internet. Although Doctors Without Borders usually does not use any form of technology other than radios while in the field, they do still make use of computers to write and submit reports and for data collection.

Doctors Without Borders or MSF (Medecins Sans Frontieres) also use their own internal accounting program that allows them to manage and keep track of the donations they receive, how they make use of that money, and how much money they need in the future. The program is only used by MSF, so they teach staff members that will be using the program how to operate it. BitEruptor had reached out to MSF regarding the security of their program by way of email, and they have yet to respond. However, based on the information provided by the HR and Finance Coordinator of MSF, Anne Kane on their website this program is meant to be "basic and simple". PayPal, a well-known online payment system company whose software does much more than just keep track of money, has been the victim of phishing attacks in more ways than one. Their costumers have also fallen prey to phishing emails as well as fake PayPal sites. Even such a successful company like PayPal lacks a security system for detecting phishing emails, so Doctors Without Borders would be benefited greatly with BitEruption.

## BITERUPTOR'S SOLUTION

By Isaac A.

Google's Chrome browser is undoubtedly the most-used internet browser with about 34.7% of internet users choosing it as their daily driver. The application has attempted to create ways to eliminate phishing attacks, however these methods do not provide the effectiveness that BitEruptor offers.

BitEruptor uses three main algorithms to tackle the spreading problem of cyber scams.

First, BitEruptor determines if a webpage may be fraudulent by the amount of spelling errors detected. If the amount of errors exceeds ten words, BitEruptor will notify the user.

Second, the program identifies possibilities of a scam by reading and processing the URL of the current webpage opened. If the domain name (take Google for example) claims to be in one of the top 100 most visited websites in America, but has an extension other than what is typically used (www.google.org instead of www.google.com, for example), the user will be alerted.

Finally, BitEruptor finds potential swindles by finding if a previous user submitted the current site as being unlawful before.

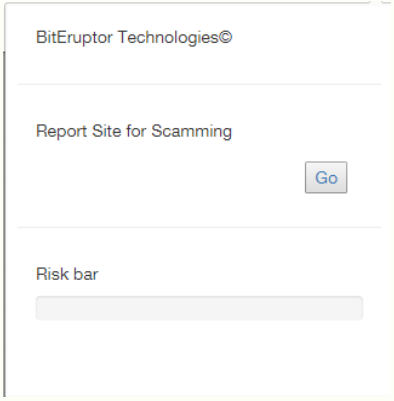
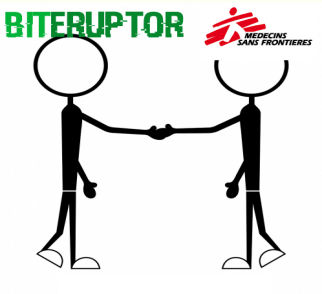



Photo Courtesy of BitEruptor

## HOW DOCTORS WITHOUT BORDERS COULD BENEFIT FROM BITERUPTOR




Stick figure drawing courtesy of 123freepictures.com. (Top Right) Logo belongs to Doctors Without Borders.

By Uialii C.

Doctors Without Borders is vulnerable, specifically to cyber scamming. This could especially hurt Doctors Without Borders because they have a monumental impact on the societies in need. The humanitarian group relies on computers for research, communication, and financial purposes, so they cannot operate efficiently if their computer system was to be shut down by hackers. Also, phishing scams may occur at any given time, and these scams could result in lost money that was initially used to make the world a better place. BitEruptor's goal is to prevent these attacks and further money loss.

Although Doctors Without Borders has not made contact with BitEruptor yet, several different organizations lack existing software for preventing phishing scams, such as Paypal. Therefore, Doctors Without Borders will most likely be in need of BitEruptor's software, BitEruption.