Media Review - Breach (2007)

While Ocean's 8 is a recent, funny, action packed, movie premiering in 2018, it showcased the importance of cybersecurity awareness within pop culture today. The plot surrounds the largest jewel heist of the century and highlights Ocean's mastermind hacker cracking through a few accounts to access a few private systems. This quick and short movement showed audiences just how easy it is to have your information compromised. In the movie, the need to gain access to a high-profile venue's camera control center. While most would think this is impossible, the movie demonstrates that this was possible with a quick phish. Doing simple research on the CEO of the security company that runs operations for The Met, the hacker was able to learn everything she needed through social media and google. The hacker then used that information to send a phishing advertisement targeted to the interest of the CEO.

> "To call this film average would be to deny its uncanny ability to entertain."
>
> *Cory Woodroof*
>
> *615 Film*

When the CEO sees the advert, he simply clicks on the link and is redirected to a page full of dog photos. This serves two purposes, the link was coded to allow the hacker to gain access to the remote endpoint and security cameras and the photos distracted the CEO long enough for the hacker to download files necessary to build the blind spot, and thus help steal 105 million dollars' worth of jewels.

Phishing attacks are designed for you, with you in mind. With the right kind of information, any email scam can look legit. Without the proper training on how to identify a phishing email from a regular email, especially if the email contains information that interests you, it's only a matter of time before you fall victim.

In hindsight, whatever anti-virus the Met was running, wasn't enough to face an "advanced attack" especially when the link didn't come through an email filter system with a file that screamed "VIRUS". It's important to highlight that without the proper security systems in place, a hack of your systems could be managed just as fast as it did in the movie.

It's also important to recognize that these same phishing attacks cost this CEO 105 million dollars. We need to remember our best practices when dealing with phishing emails and make sure to use them daily.

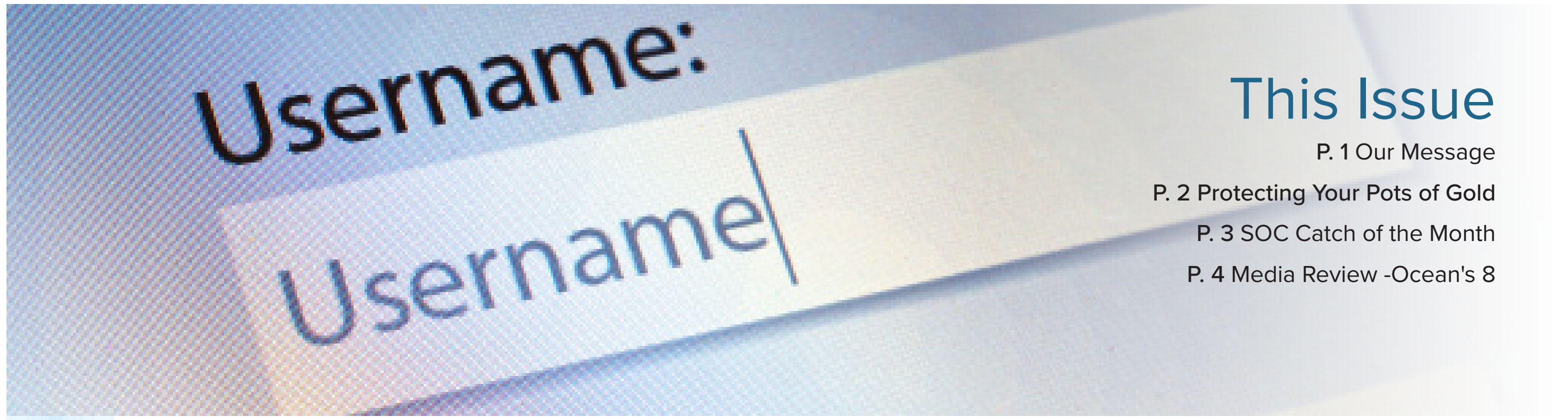
CONNECTIONS

Connect with us on social media

Call us at
808.206.8549
or email us at
info@hitechhui.com

March 2022
Volume 45

HITECHHUI NEWSLETTER



This Issue

> *" For purposes of action nothing is more useful than narrowness of thought combined with energy of will."*
>
> *– Henri Frédéric Amiel*

OUR MESSAGE

Protecting Your Pots of Gold

The first few minutes of 2022, I felt anything but lucky! It was right before the countdown to 2022 and while everyone around me was celebrating preparing for a new year (hopefully the end of Covid and other great things), I was on the phone with the fraud department at my bank.

I was looking over expenses in my bank and I noticed a check that was taken from my account that didn't look quite right. It seemed like it could have been a legitimate transaction, except – it was one we didn't make! In fact, a scanned copy of the check showed that it was almost identical to my real checks with just a slight change in the spelling of my name. Someone had created a counterfeit of our checks, forged a signature and successfully used it! Yes, cashed in and all! My pot of gold, gone.

With our little use of checks, four checks written from that account in 2021 and two of them written to ourselves, I have no real idea how they got a copy of ours to duplicate it. I was shocked!! After some research, I learned there was a market on the darkweb for check info. With a copy of a check anyone can duplicate and cash in, steal your identity and more.

We can only assume that one of the 2 companies we wrote the checks to in Hawaii, sold my details to someone in California and cashed it at a Wells Fargo bank. The most terrifying part of this, is the bridge that crosses old school theft into financial cyber crime and identity theft. Unfortunately, criminals will stop at nothing to steal your gold no matter where you've stored it, or how you spend it.

Reported cases of situations like ours, show that in addition to changing payee and amounts of checks, criminals are selling a copy of your check for a few hundred dollars on the black market. Buyers are then using the checks to steal the victim's identity by using their name and address to manufacture fake driver's licenses, passports and other legal documents. They can also use this information to boost their phishing attempts to you and your employees by having a large amount of accurate data to present to create a false sense of security.

We talk a lot about phishing attacks, emails being used to gain information to steal financial accounts, credit cards, and other payment card information. We think it's incredibly important to have all your employees trained routinely on current tactics and attempts criminals are using to steal your data and money. A ransomware attack alone can cost businesses hundreds of thousands of dollars to recover, let alone a ransomware attack coupled with financial fraud.

While there's little to do to prevent the physical fraud (other than to avoid sending checks), here are a few things to keep in mind.

1. Protect checks that you give out and the checks that come to you. Only have a minimum number of people handle checks.
2. If you use remote deposit, shred checks after 2 weeks.
3. Have checks and balances, double check every check that comes out of each and every one of your accounts.

Stay safe out there, and remember, you create your own luck!

- Chuck Lerch

SHINY NEW GADGET OF THE MONTH

The LINK AKC Smart Collar

The world can be a dangerous place for a pooch who doesn't know any better; so, it's best to know how to keep tabs on your canine companion in case they bolt. That's where the LINK AKC smart collar comes in.

This smart collar is a comfortable and safe tracking alternative for your pooch. The LINK AKC smart collar comes equipped with several other useful features, including but not limited to:

- Activity monitoring and sound training specific to your dog's breed
- Temperature alerts if your dog is too hot or cold
- A place to digitally store vet records
- Waterproof features for up to 30 minutes in three feet of water If you want your dog to be the goodest, highest-tech boy or girl out there, this collar is for you!

Don't Leave It To Luck When Educating Your Team About Phishing Attacks

No company is immune to phishing exploits… it's inevitable that one of your employees will unknowingly click on a link in an email and expose your company's network and data to threat actors looking for a vulnerability and do some serious damage. That will cost your company time and resources to identify and remediate - a cost that is entirely avoidable.

Phishing, is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. Every day, we are inundated with emails that may contain malicious content and result in security breaches that will wreak havoc on company networks. Training employees is key to providing a line of defense at the entry point of malicious content sent by phishing emails.

DID YOU KNOW?

- CISCO's 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86% of organizations and suggests that phishing accounts for around 90% of data breaches.
- According to a study by IBM, human error is the main cause of 95% of cyber security breaches.
- 91% of successful data breaches started with a successful spearfishing attack (KnowBe4 - 2021)
- Benchmarking performed in 2020 by KnowBe4 revealed that there were "radical drops in careless clicking after 90 days and 12 months of simulated phishing testing and security awareness training." (Phishing by Industry 2020 Benchmarking Report)
- Average time for data breaches to be identified and contained - 287 days (2021IBM Cost of a Data Breach Report)
- Average cost to fix a data breach $4.24 million USD (2021 IBM Cost of a Data Breach Report)

THE HUMAN FACTOR

No matter how much you try to protect your endpoints with tools and monitoring, one thing that isn't necessarily covered by sophisticated cyber protection tools, is the human factor. Face it - more than ever, employees are super busy, multi-tasking, working from home, buried in emails - and it's easy to click on a link, in haste, that looks innocent enough. How do we address this human factor? Education and awareness training is first and foremost to improve security awareness - but is it enough?

Enter KnowBe4 - provider of the world's largest security awareness training and simulated phishing platform.

In addition to their comprehensive security awareness training platform, KnowBe4 provides an innovative and effective solution to test your employees' security awareness through phishing simulation tests and analytics.

Some of the key features of KnowBe4's phishing simulation program include:

- Over 12,000 email templates to send to your employees; send them as-is or customize
- The ability to customize and schedule targeted emails campaigns
- Meaningful reporting to identify areas of concern (i.e. trending for individual departments, employees who have a history of clicking and categorization of their behaviors)
- Risk scores at the individual user level that management can use for training purposes
- Benchmarking data so you can compare how you rank against similar companies in your industry

EFFECTIVENESS AND RESULTS

Phishing simulation tests using real-world examples is an effective way to understand human behaviors in your company and KnowBe4 has the data so management can act on these patterns of behavior. Once employees click on the links in the email, they are immediately notified that email was a phishing test and red flags in the email are highlighted to show what they should have looked closer at to identify the phish. If used in conjunction with KnowBe4's security awareness training platform, additional training will be recommended for the user.

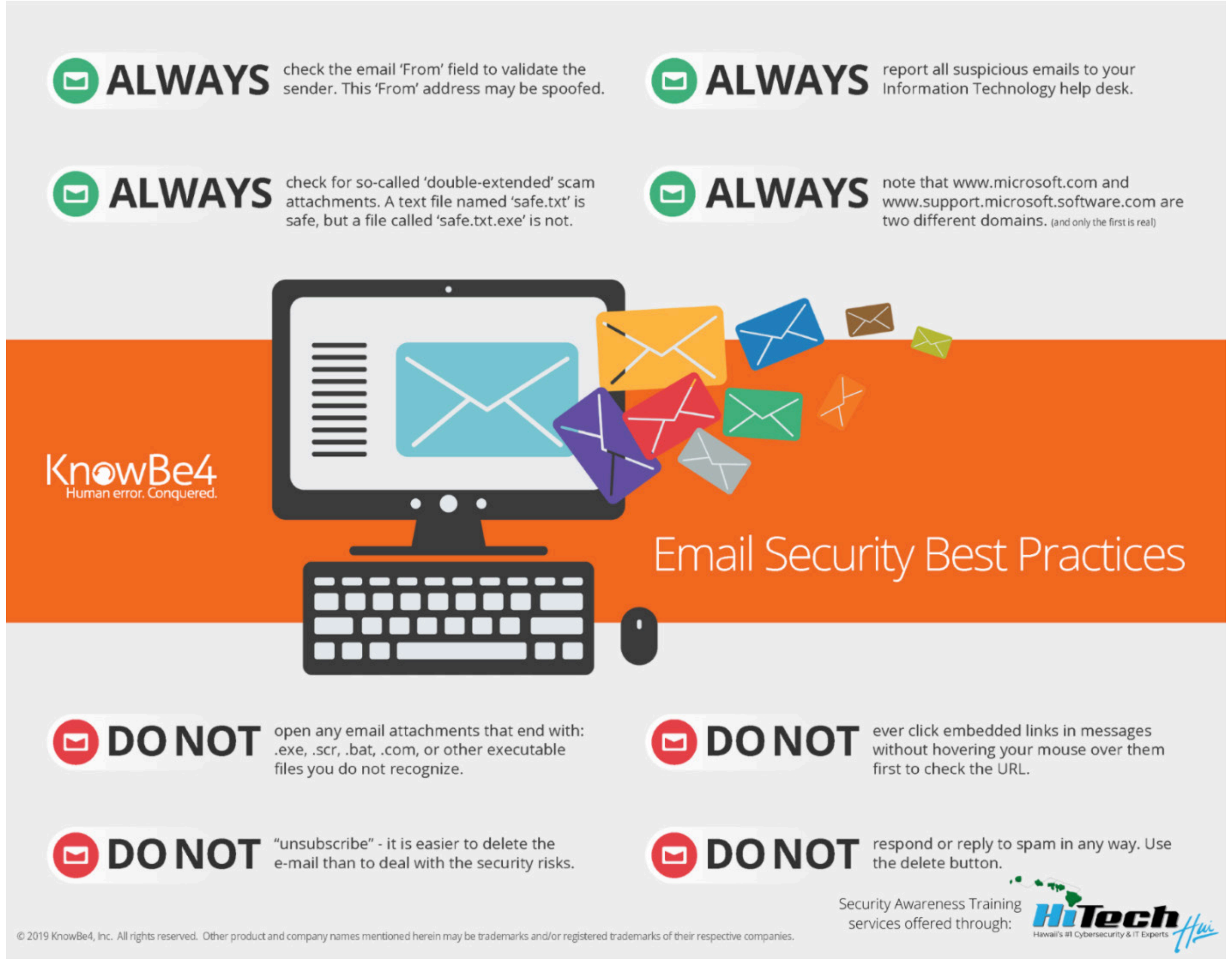
Based on stats compiled by KnowB4 from their clients - here is how effective phishing simulation testing is:

- 31% of users clicked on the link in the email after first phishing simulation test.
- 16% of users clicked on the link in the email tests sent three months later.
- 5% of users clicked on the email tests sent twelve months later

These results demonstrate the effectiveness of testing, and after twelve months, the decline in the numbers of employees who clicked the link in the email is indicative of an improvement in an organization's security culture. This will translate into improving your company's risk posture when it comes to this last line of defense when it comes to phishing - your employees.

Reach out to us at HI Tech Hui for more information about KnowBe4 and to better understand the human factor when it comes to mitigating security breaches.

KnowBe4



ALWAYS check the email 'From' field to validate the sender. This 'From' address may be spoofed.

ALWAYS report all suspicious emails to your Information Technology help desk.

ALWAYS check for so-called 'double-extended' scam attachments. A text file named 'safe.txt' is safe, but a file called 'safe.txt.exe' is not.

ALWAYS note that www.microsoft.com and www.support.microsoft.software.com are two different domains. (and only the first is real)

KnowBe4
Human error. Conquered.

Email Security Best Practices

DO NOT open any email attachments that end with: .exe, .scr, .bat, .com, or other executable files you do not recognize.

DO NOT ever click embedded links in messages without hovering your mouse over them first to check the URL.

DO NOT "unsubscribe" - it is easier to delete the e-mail than to deal with the security risks.

DO NOT respond or reply to spam in any way. Use the delete button.

Security Awareness Training services offered through: HiTech Hui Hawaii's #1 Cybersecurity & IT Experts

OUR SOLUTIONS

Cyberuptive
FIREEYE
SOPHOS
Fidelis Cybersecurity
BlackBerry CYLANCE
JUNIPER NETWORKS
proofpoint
datto
backupify
DEMISTO
thycotic
CISCO
Microsoft 365 Business
bitglass
Qualys
paloalto NETWORKS
DUO
KnowBe4