**Presentation: Cyber Security Best Practices for Tech Based Events and Video Conferencing Tools like Zoom, Google, Facebook Live etc**

**Date: May 23rd**

**By: Leonard Oshiyemi**

**Abstract/Introduction:**

According to Bill Gates, if your business is not on the internet, then your business will be out of business. And to be on the internet you will need to protect your business online which is what cybersecurity is all about.

Cybersecurity has been a hot topic as of late with protocols being developed across a slew of industries, from automotive innovation to the medical field. As a new decade begins, it is more important than ever to be aware of new threats and how to fight them — as well as the repercussions of being left in the dust if you decide to do nothing about it.

As technology evolves, so does the way we do business around the globe — but as the world continues to become more digital, computer hackers continue to come up with new ways to steal our data. However, even with that knowledge, companies and individuals remain not fully aware of the magnitude of the threats of cybercrime, and this is the time for a learn more about in order to do something about it.

**Facts about Cyber Security**

* 95% of breached records came from only three industries in 2016 – Government, retail and technology.
* There is a hacker attack every 39 seconds
* 43% of Cyber Attacks target small businesses
* In 2018 hackers stole half a billion personal records
* 95% of cybersecurity breaches are due to human error
* More than 77% of organizations do not have a cyber security incident response plan
* Most companies take nearly 6 months to detect a data breach.
* Total cost for Cyber Crime committed globally has added up to over $1 trillion dollars in 2018
* The average cost of a data breach in 2020 will exceed $150 million.

So if you think that you are immune to this attack please think again.

## Remember the Basics

As earlier stated, cyberattack occurs every 92 times in every hour, with companies getting the brunt of these dangerous attacks. That means that no matter the size of your business, it is essential that cybersecurity basics are implemented to avoid a potential disruption. Further, for some businesses, the protection of private records is not only ethical, it is the law. For instance, the health industry must comply with the WHO and Ministry of Health guidelines that states that it is the responsibility of the company to protect the information of their patients.

This is important for every other business as well because protecting the information of your customers must be a top priority, and if you do fall victim, then your company could be on the hook for hundreds of thousands of dollars in damages. Because of this, it’s imperative that you teach everyone in your company the basics of cybersecurity. Start by having them log in with complicated passwords that include numbers, letters, and symbols. For extra secure content, employ two-factor authentication where an employee must enter a code from an external device in addition to their password.

A common threat for businesses and individuals alike is still the phishing email. In this type of attack, a hacker gets a hold of your email address and then sends an email that seems to be from a trustworthy source like a doctor or a bank, and usually contains a malicious link or attachment that, when opened, provides a doorway for the hacker into your system. Once inside, the hacker can release ransomware, which takes your data hostage and demands payment in exchange for release. The best way to prevent phishing attacks from getting the best of your business is through proper training of your workforce.

## Building a fortress

As technology continues to advance, so will the methods that hackers use to break into businesses. To protect against this, create a force field around your company with simple but efficient tech tools. Start with a secure firewall, from which there are many types to choose from. The more popular options are packet filtering firewalls, which compare small pieces of data to see if they are safe and then only keep the good stuff. There’s also a proxy firewall, which monitors all information that goes in and out to verify its legitimacy. Install a firewall and then update the software every time there is a new version to protect against new vulnerabilities.

Another layer of your cybersecurity fortress should be a virtual private network, or VPN. Essentially, a VPN allows you to connect to your company’s network — but when you do, you go through a server that might be located somewhere else around the world, so it appears that you are browsing from there rather than your true location. This is especially important for businesses with remote employees who want to connect to the central servers. A VPN creates more work for hackers, so they are less likely to intrude directly into your networks.

As we venture into 2020, more businesses will be utilizing remote employees, on top of the growing trend known as BYOD, or Bring Your Own Device, which has employees using their tablets and smartphones in and out of the office to conduct business. However, these independent devices need to be protected, as well. To protect your business and customer data, devices should be updated regularly and secured with passwords. If employees work from public places, they need to be wary of public Wi-Fi, as hackers can employ a man-in-the-middle attack, which is a fake Wi-Fi network that, when connected, allows the hacker to steal info from the device.

## Blockchain and cryptocurrency

## What are Blockchain and cryptocurrency technology?

These trend setting are gaining steam as the years go by is the use of cryptocurrency and blockchain technology for businesses and their customers. In a nutshell, cryptocurrency is an electronic currency that is made up of bits of data instead of dollars and coins. Cryptocurrency is held and used via electronic wallets that use a complicated key-system to keep the wallet secure.

Partnered with cryptocurrency is a blockchain, which is literally a series of connected blocks of user data or currency transactions that can only be modified by the owner because they are bound by cryptography, or mathematical, rule-based calculations. The long and the short of it is that many industries are starting to get into the blockchain game in order to further secure the records of their customers.

The healthcare industry is even jumping on the blockchain bandwagon to protect patient records. Depending on the patient’s ailments, their personal and medical information might be passed from doctor to doctor, specialist to specialist, so when their data is transferred utilizing blockchain, the patient has total control over how their records are changed and adjustments cannot be made without the owner’s permission.

The banking industry is also utilizing blockchain technology to make global payments from country to country easier and more secure while saving money as the transfer is almost immediate, and there are fewer traditional banking fees. However, as with any new technology, there are still security concerns.

The only thing keeping blockchain and cryptocurrency wallets secure is a private key, which the owner of the blockchain possesses. While the key is usually very complex with a string of multiple words or letters, it still has to be remembered. Users who are less aware of cyber threats may store this key within the files of their computer, and if they are hacked, the hacker could potentially locate the key and would then have full access to the victim’s money. With that in mind, more time and research are necessary to fully believe in the security of blockchain technology.

## Training Remote Employees About Your Cybersecurity Policies

As the world swiftly adopts the remote-work trend, employees should understand the repercussions of choosing convenience over security. Sacrificing security is not a pleasant tradeoff.

To illustrate this, PCMag surveyed 1000 employees about how they access corporate networks while on vacation. The results were scary. 77% agreed to have connected to free public Wi-Fi networks, and only 17% said they use a secure VPN to operate their corporate computers and phones.

To make matters worse, 50% of employees aren’t aware of their remote-work cybersecurity policies.

If you own or manage an enterprise, be sure that you establish out-of-office guidelines along with in-office rules. If you already have security guidelines, be sure to remind employees about using them periodically.

## Practicing Cyber-Hygiene Habits

With organizations falling prey to an unprecedented number of phishing attacks and cyberattacks, performing elementary security processes can go a long way. Here are a few cyber-hygiene habits that can help.

* Ensure that your routers and firewalls are deployed and properly configured.
* Keep updating whitelisted and blacklisted user lists at regular intervals.
* Enforce compartmentalized user permissions for authorized users.
* Keep antivirus definitions up-to-date.
* Run vulnerability scans and update OS with the latest security patches.
* Backup and encrypt business data.
* Enforce strong password policies and 2FA/MFA procedures.

## Using Multi-factor Authentication

When it comes to cybersecurity best practices, experts often list multi-factor authentication (MFA) in the top five. The reason has to do with how MFA offers more than one form of authentication.

**And this is how it works…**

Let’s assume that you want to log in to an account that has an MFA setup. You cannot just get in with your username and password. The account server will ask you for a second form of authentication before actually letting you in.

For an example consider what it’s like when you open a bank account. When registering for an account, you’ll need to provide a picture ID, along with another form of identification (like your passport or SSN). That extra layer of security used at banks is similar to how MFA works.

These cybersecurity best practices will go a long way to helping you secure your data. It’s wise for every business to follow them. After all, the cost of losing sensitive data is much higher than the cost of prevention.

**Now Let’s Go into Conferencing Tools Best Practices**

The importance of Video conferencing technology can never be over-emphasized. This new medium now makes our conversation and online meetings more fluid and easier even pre-COVID-19 era. In this COVID-19 era, these apps have grown in leaps and bounds to ensure that we continue to have seamless meetings anywhere in the world. The major players are Zoom, CISCO Webex, ClickMeeting, Microsoft Teams, GoToMeeting, Google Meet, CyberLink U Meeting, BigBlueButton, Bluejeans Meetings, Lifesize, RingCentral Video etc.

Just like a normal meeting, this can take our businesses to the next level. However, as good as this may portends and just like a motor vehicle if not used properly it could lead to a disaster.

So that being said, these are what we put together as the golden rules/best practices for one to have a successful video conferencing outing generally across all the platforms….

1. **Proper Lighting** – Putting a shining light on an item makes the item glows. So the same is applicable here. So to look your best, ensure that you put the light facing you just like they do to celebrities on TV. Avoid putting the light behind you or from a window or directly overhead.
2. **Proactively prevent Technical Difficulties** – Make sure that you arrived about 10 mins early before your meeting to ensure that the microphone, speaker of your computers or laptops are working. The system may need you to install something like a system update or any of the annoying Microsoft patches.
3. **Strong Internet connection** – A strong connection will not only give you a piece of mind but will also keep you in the meeting and prevent you from falling in and out of the video call. Nothing is as bad when you are like 2 seconds delay lag behind the rest of the team or having to stare at a frozen screen while others are contributing in the meeting. If you are using a mobile wifi, look for a suitable spot in your house or wherever you are in order to have a good reception or connection.
4. **Position Yourself in the Center of the web cam** – Look inside your computer screen like a frame and you want to be up front and center. So you need to sit upright with your upper body showing with a smile on your face.
5. **Always make eye contact** – It’s important to engage with the person on the other end of the line. It’s imperative to look them in the eyes and make a real connection – this will help you build trust and form a lasting relationship. So position yourself for better camera placement and make eyes contact.
6. **Refrain from munching** – Don’t eat or chew gum or even be drinking your favorite tea or coffee. If you won’t bring that tuna sandwich, or shawarma or Burger or the steamingly hot pounded yam or Kenke or Banku into a meeting with your boss, then don’t bring it into a video call. Though they can’t smell it, but it can be very distracting and come off as disrespecting.
7. **Don’t Pull a Disappearing Act** – If you are working from home and you must step away in video call meeting, you need to notify the group by politely excusing yourself verbally or in the video conference call.
8. **Don’t send inflammatory text messages** – Zoom has a text messaging capability but this messaging has got so many people who were exchanging derogatory and unpleasant messages in trouble about their bosses who ended up seeing the transcript of the messages when the video call meeting was concluded. Rule of thumb, don’t send any messages that you don’t want anyone else to see. There is no privacy really.
9. **Keep Movement to a Minimum** – There are some bad habits like tapping the table, chewing on the pencil, kicking the chair or the tables should be kept to the minimum as these could cause great distractions to people on the call.
10. **Keep a professional** **background** – This goes for not only noises but also visuals. A messy room, your kids or pets running around or a bustling coffee shop behind you can also be distracting for participants. That’s not saying that you can’t or shouldn’t have anything behind you, you could have a nice piece of painting, colorful wall or neatly ornamented shelves with your personal touch could say a lot or go a long way. For instance, there was an incident making rounds on Social Media where the wife was having a video conference call and the husband was coming out of the shower naked behind her. What an embarrassment for her, her family and her colleagues. This could have been avoided if the wife had kept and chosen a professional background.
11. **Remember to include all participants** – This is mostly for the moderator of the call as this could be a meeting of people in different multiple locations. So it’s important to ask all participants especially those that didn’t say much, if they have anything they would want to add.
12. **Mute your call when you are not talking** – We’ve been there before when you think that you have muted or that everyone has left the call and boom you said something that you shouldn’t have said. This can be incredibly embarrassing or can even get you in trouble.
13. **Dress to kill** – Looking good is a good business. See this as an opportunity to step up your fashion game even if you work in a casual office setting. See your video conference as an interview session where you are making a very first and good impression. Even if you are working from home and you have pajamas on the bottom. Just don’t get up in the middle of the call and ensure that you have a good professional top on.
14. **Avoid Typing –** So stop typing when on vid call. This does not only creates a distraction but also implies that you are not fully engaged or paying attention. Even if you are going to type, so just pick up a good old pen and paper in order to save the other attendees the annoyance from your keyboard.
15. **Use a good angle to position your image properly** – Just like having a good angle in a photo, you need to have a good angle in video call as well to look right. The closer to the eye-level and front-facing, the more it will look like you are talking directly to the person on the end of the call. If you are seated at a desk, this is usually propped up and slightly angled down. The closer to the chest height the better.

**Now we onto Zoom’s Specifics**

**Zoom Cool Features**

1. Meeting Recording is a cool feature to have, but be careful because this would end up in the cloud somewhere and some people can get access to it. So ensure that confidential items like the intellectual properties, trade secrets, espionage etc are not discussed or recorded on this platform. Or betterstill opt to store the recording on your local drive, which is your computer hard-drive.
2. Limit sensitive documents or files that you share inside zoom meetings. These documents could end up been stored in some storage severs somewhere in China and you know that the Chinese govt has the right to see everything stored within their jurisdiction.
3. Zoom also stores data about your operating system, IP address, location, and device for every meeting you attend, and makes this information available to your company admins. For instance, if you had told your boss that you were in London and Zoom reported otherwise. So you can see that trouble is on its way.
4. Don’t believe in Zoom’s advertised end-to-end encryption - Zoom gained its market share not only for its prices and feature set, but also because it touted the product’s end-to-end encryption. With end-to-end encryption, all communications between you and the people you’re calling are encrypted in a way that only you and the people on the call can decrypt them. All other parties, including the service providers, cannot. Sounds cool, but it’s next to impossible, as security researchers have pointed out. Zoom had to acknowledge that in its case, the other end means the Zoom server — meaning the video is encrypted, but Zoom employees, and potentially law enforcement agencies, have access. The text in chats, though, seems to be really encrypted end-to-end. The encryption fudging is not necessarily a reason to abandon Zoom for good — other popular video conference services lack end-to-end encryption as well. But you should keep it in mind and avoid discussing personal or trade secrets on Zoom.
5. Zoom had also been using Chinese data centers to route users calls. Normally, Zoom calls are routed through local servers. But because of the recent surge of traffic, Zoom has been routing traffic through backup servers that are not geographically near the users. And some of these servers were located in China. This is problematic because China does not have strict data privacy laws, and the government could demand that Zoom hand over these data from those servers anytime.
6. And if you signed up onto Zoom with an institution-specific email (not Gmail, Hotmail or Yahoo) for example with [loshiyemi@hoffenheimtechnologies.com](mailto:loshiyemi@hoffenheimtechnologies.com) email, everyone who signed up with the same email domain will get access to your full name, email addresses, profile picture, and online/offline status. So be careful of this. This is a privacy issue.
7. Use your work e-mail to register with Zoom - A weird glitch in Zoom (which at the time of this writing wasn’t yet fixed) causes the service to consider e-mails of the same domain — unless it’s a really common domain such as @gmail.com or @yahoo.com — as belonging to one company, and it shares their contact details with each member of that group. For example, that happened to users who registered Zoom accounts using e-mails ending with @yandex.kz, which is a public e-mail service in Kazakhstan, and it may happen again with e-mail addresses belonging to smaller public e-mail providers.

So, to register with Zoom, use your work e-mail. Sharing your work contact details with your real colleagues should not be a big deal. If you don’t have a work e-mail, use a burner account with a well-known public domain to keep your personal contact details private.

1. Don’t fall for fake Zoom apps - As Kaspersky security researcher Denis Parinov discovered, this March the number of malicious files incorporating the names of popular video conference services (Webex, GoToMeeting, Zoom, and others) in their filenames had roughly tripled in comparison with the numbers he found month by month over the previous year. That most likely means malefactors are ramping up their abuse based on the popularity of Zoom and other apps of its kind, trying to disguise malware as videoconference clients. Don’t fall for it! Use Zoom’s official website — zoom.us — to download Zoom safely for Mac and PC, and go to the App Store or Google Play for your mobile devices.
2. Don’t use social media to share conference links - Sometimes you want to host public events, and in many places online events are the only type of public events available these days, so Zoom is attracting more and more people. But even if your event is truly open to everyone, you should avoid sharing the link on social media. If you knew anything about Zoom before reading this post, you’ve probably heard about so-called Zoombombing. It’s a term Techcrunch journalist Josh Constine coined to describe trolls disrupting Zoom meetings with offensive content. Right now, several chats on Discord and threads on 4Chan (both popular with trolls) are discussing targets for their next raids. Where do the trolls get information about upcoming events? That’s right, they find them on social media. So, avoid publicly posting links to Zoom meetings. If for some reason you still want to, make sure you don’t enable the Use Personal Meeting ID option.
3. Enable Waiting Room - Another setting that gives you more control over the meeting, Waiting Room — recently enabled by default — makes participants wait in a “waiting room” until the host approves each one. That gives you the ability to control who joins your meeting, even if someone who wasn’t supposed to participate somehow got the password for it. It also lets you kick an unwanted person out of the meeting — and into the waiting room. We recommend leaving this box ticked.

**How to Protect Your Meetings and Accounts**

1. Protect every meeting with a password - Setting up a password for your meeting remains the best means of ensuring that only the people you want in your meeting can attend it. Recently Zoom turned password protection on by default — a good move. That said, don’t confuse the meeting password with your Zoom account password. And like meeting links, meeting passwords should never appear on social media or other public channels, or your efforts to protect your call from trolls will be in vain.
2. Protect your account - A Zoom account is just another account, and in setting yours up, you should apply the basics of account protection. Use a strong and unique password, and protect your account with two-factor authentication, which makes your account harder to hack and better protected, even if your account data leaks (though so far that hasn’t happened).

There’s at least one more Zoom-specific catch: After you register, in addition to your login and password you get a Personal Meeting ID. Avoid making it public. And because Zoom offers an option to create public meetings with your Personal Meeting ID, it’s quite easy to leak that ID. If you do, anyone who knows your PMI can join any meeting you host, so share this information prudently.

1. Pay attention to screen-sharing features - Every normal videoconference app offers screen-sharing — the ability of one participant to show their screen to the others — and Zoom is no exception. Some settings that are worth keeping an eye on: Limiting screen-sharing ability to the host or extending it to everyone on the call. If you don’t need other people to show their screens, you know which option to choose;  
   Letting multiple participants share screens simultaneously. If you can’t immediately see why your meetings would need this capability, you’ll probably never need it; just keep it in mind in case you ever need to enable it.
2. Stick with the Web client if possible - The various Zoom client apps have demonstrated a variety of flaws. Some versions let hackers access the device’s camera and microphone; others let websites add users to calls without their consent. Zoom was quick to fix the aforementioned problems, as well as other, similar ones, and it stopped sharing user data with Facebook and LinkedIn. However, given the absence of a proper security assessment, Zoom apps likely remain vulnerable, and they may still employ shady practices such as sharing data with third parties. For this reason we recommend using Zoom’s Web interface instead of installing the app on your device, if possible. The Web version sits in a sandbox in the browser and doesn’t have the permissions an installed app has, limiting the amount of harm it can potentially cause. In some cases, however, even if you want to use the Web interface, you may find that Zoom has gone ahead and downloaded the installer, and there’s just no other option to connect to the meeting but to install the client. In that case, you can at least limit the number of devices on which Zoom is installed to just one. Let it be your secondary smartphone or, say, a spare laptop. Choose a device with next to no personal information. We know that sounds somewhat paranoid, but better safe than sorry. By the way, if your company already uses Skype for Business (previously known as Lync), then you have another option. Skype for Business is compatible with Zoom and can handle Zoom conference calls just as well — without the aforementioned flaws.
3. Think about what people can see or hear - This one applies to every videoconferencing service, not just Zoom. Before you jump on the call, take a moment to consider what people will see or hear when you join the call. Even if you’re home alone, they may expect you to be fully dressed. Basic grooming is probably a good idea.

The same holds true for your screen if you plan on sharing it. Close any windows you wouldn’t want others to see. Whether it’s a surprise gift you’re buying online for another person on the Zoom call or a job search your boss doesn’t need to know about. And on this note, I conclude and I say a big thanks for having me.

**End**

**Questions Time…**