LOGICAL TALK · OCTOBER 2020 EDITION

WHAT'S NEW?

In our September issue, we had announced the formation of our Customer Service Experience Team. One of the things we have put together in the last two months is developing our common purpose to deliver quality customer service consistently.

Moving forward, our company will operate on one common goal, which is ***"To make our customers feel Heard, Helped and Happy."***

ABOUT THE AUTHOR

This monthly publication provided courtesy of Andre Vittorio, President of Idealogical Systems Inc.

Our Mission:

To build a community of successful- minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

It's Cyber Security Awareness Month 2020 Is the Year of Zero Trust Framework

We already know it is bad to have a username and password hacked but worrying about securing all your personal and work credentials is a little overwhelming. As a result, we naturally slack at being cautious about the protection of our credentials.

This behaviour acts as a feeder for hackers and botnets, which is why they were able to attack 71% of Canadian businesses in 2019.

Therefore, the one defense mechanism that you can rely on is the Zero Trust Cybersecurity Framework.

What is Zero Trust Cybersecurity Framework?

Zero Trust is a strategic approach to cybersecurity based on "Never Trust, Always Verify." Zero Trust is designed to simplify granular user-access controls, offer complex threat prevention (Layer 7 threat), and leverage network division.

A Zero Trust security framework helps you prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through your network. For example, if a co-worker asks you for any work asset via email or phone, you must verify their trustworthiness before sharing the said work asset.

Why is Zero Trust Cybersecurity Framework In 2020?

Continued on page 2

Continued from page 1

A recent study by Information Systems Security Association (ISSA) and independent industry analyst firm Enterprise Strategy Group (ESG), states that "The COVID-19 pandemic has presented a once-in-a-lifetime opportunity for hackers and online scammers." The cybersecurity professionals saw a 63 percent increase in cyberattacks related to the pandemic.

The most alarming discovery from the study is that 20% of global security experts believe that businesses will increase their security spending in 2020. At the same time, 25% of experts think that the pandemic's challenges will force businesses to decrease their security spending this year.

Like ransomware attacks, most attackers' aim is disruption; and with more people continuing to work remotely than ever before and all requiring access to virtual corporate networks, sustaining access is vital to the day-to-day operations of businesses.

This is aiding hackers with an opportunity to run extortion campaigns against companies and their critical services, during which they can threaten to take control of your systems unless a payment is made. Perhaps one of the biggest concerns around some of the recent most sophisticated attacks is that they're relatively easy to carry out, even for low-level attackers.

> **"The COVID-19 pandemic has presented a once-in-a-lifetime opportunity for hackers and online scammers "**

Here are some security guidelines for employees who are working from home for the rest of 2020

Home Wi-Fi: Ensure your home Wi-Fi connection is secure. While most Wi-Fi is correctly secured, some older installations might not be, which means people in the near vicinity can snoop your traffic. Additionally, change your Wi-Fi name and password every 15 days.

Security Updates: Your third-party apps like Microsoft, WhatsApp, Zoom, etc. sends regular updates for your apps. Ensure all your laptop and mobile apps are patched and updated regularly.

Lock Your Device: Lock your screen when your devices are unattended within your home. The chances of hackers gaining access to an unlocked screen are higher than a locked screen. This applies to smartphones, tablets, laptops and desktops.

Backup Regularly: Ensure all your files are backed up regularly. In a worst-case scenario, if you fall for a foul of ransomware, for instance, you will have a back-up of your files and won't lose your data.

Idealogical's High Happiness Quotient: Customer Satisfaction Survey

To be true to one of our 10 core values 'Honesty & Cooperation', we introduced a new ONE CLICK satisfaction survey for our end users. And the results are gratifying.

In September, our customer satisfaction response rate was 73.4%, which is 30% higher than the industry average. We achieved a customer satisfaction score of 88.4%, which is close to our goal of 90% and higher. And our happiness score was 92%, which means 206 out of 224 respondents were happy with our service.

We encourage you to continue giving your feedback and promise you to continue improving the quality of our customer service.

How to Be A Happiness Hero in Customer Service
by Ian Chauhan

Photo: Ian Chauhan in his earned swag from our happy clients - Willard Meats.

Growing up, I spent a lot of time at my dad's factory, giving him an extra hand at his commercial dry-cleaning business. One of the things I remember the most is how friendly my dad was with his customers. He knew everything about them – right from where they got their thanksgiving turkey this year to what grade their kid is graduating to. I remember smiling every time they would chat about something silly.

My dad has customers who have been with him for over 30 years now. One of the reasons I think my dad was able to do that was because he takes time to get to know his customers as he would with his friends. I guess I have adopted the friendliness of my dad with his customers to my work in IT.

The difference between my dad and my line of work is that at the Idealogical helpdesk, clients always call us in distress – when something is not working. But, taking their mind off work while I am working on resolving their issues is how I am able to turnaround my interactions with them.

The best interaction that I have had with our clients has never been about work. Yes, I have a job to do, but if I can do it while I get to know the person on the other side of the line, then why not?

I enjoy working at Idealogical because one of our core values is "We have fun always," which aligns with my value: working with people or for people is not fun when it's all about work.

Customers enjoy speaking with us at Idealogical is not just because we are good at what we do, which is 'we take away their IT headaches,' but we also make an effort to build a relationship with everyone we interact.

Actor Erwan McGregor once said, "You've got to look after the relationships

in your life, and if you don't, you're losing something very important". His words have been stuck with me ever since.

Intentionality is something that we talk about a lot at Idealogical. As an IT professional, my intent isn't just to fix clients' technical issues, that's just my job, but building relationships is what I focus on the most. Striking a conversation where there is a friendly dialogue, the work gets done faster in the most pleasant way.

I firmly believe that every time one makes an extra effort to get to know a person or their issues, they will feel heard. Every time you put in a little more effort to help them resolve their issues, they will feel helped. And, every time you put an extra effort into getting to know somebody, they will feel happy. I apply this to both my professional and personal life.

This Halloween Don't Go Trick or Treating with Hackers: Invest in Employee Education On Cybersecurity

According to a 2019 study by IBM, human error is the leading cause of 95% of cybersecurity breaches. This means, 19 out of 20 cyberattacks in 2019 could have been prevented if human errors were eliminated from the equation.

What is a human error in IT security?

In the context of IT security, the human error means unintentional actions - or lack of action - by employees and users that cause, spread or allow a security breach to take place.

What are some examples of human errors in IT Security?

There is an endless number of human errors that could significantly increase risk and compromise a business. Some of the common ways are:

Setting up non-complex passwords or reusing the same password for more than one application.

Delay in installing the security updates on their phones, laptops and desktops

Sending something to a wrong recipient - is a common threat to corporate data security; misdelivery is the fifth most common cause of cybersecurity breaches.

How to prevent human error in your business?

Eliminating the opportunity and the event that puts a business at risk is an option. But it also falls under the category of being a little too optimistic.

The strategic answer is consistently Education & Training your employees.

End-users will continue making mistakes if they don't know what the correct actions are and what the risks are. To breach this gap, it is essential to approach human error from both sides to create a comprehensive defence for your organization.

Educating your employees on security basics and best practices allows them to make better decisions. It enables them to keep security on their minds and seek further guidance when they're unsure what the consequences of a specific action are.

Training your employees on security topics that they may encounter in their day-to-day work activities is essential. Whether it is basic topics like email hygiene, safe use of the internet and social media do's and don'ts or complex subjects like phishing, ransomware and malware, your employees should be aware.

Humans don't have to be the weakest links. You can reduce human errors with effective security awareness training.

Contact us at ideas@idealogical.com to schedule a cybersecurity training session for your employees.

Tony Hsieh: The CEO Who Picked Culture Over Bottom-Line

A Harvard graduate and a son to an American working-class family, Tony Heish is an entrepreneur who sold his first business, LinkExchange, to Microsoft in 1998 for $265 million. Later, he invested in a shoe e-commerce company Zappos which has passed $1B in sales and acquired by Amazon in 2009.

The secret to Tony's success is building a business with well-defined core values and strong company culture. He affirms that "The reason most companies don't focus as much as they should on customer service or company culture is that the ROI is usually 2-3 years down the line." Thinking long term, companies can get the culture to drive customer service, engaged employees and create a great brand.

August 2020, Tony announced his retirement to focus on philanthropic work.