idea LOGICAL

LOGICAL TALK · NOVEMBER 2020 EDITION

WHAT'S NEW?

At Idealogical, we are constantly trying to improve our customer service approach. Keeping that in mind, we are proud to announce that we are launching another way for our clients to reach our Helpdesk with LIVE CHAT.

Starting this month, you will be able to open a service ticket via Chat. That means, now, you can reach Idealogical Helpdesk by phone, email, online portal and LIVE CHAT.

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.

Phishing Attacks: How to Recognize Them and Keep Business Data Safe

Cybercrime is on the rise, and hackers are using any opportunity to take advantage of an unknowing victim to gain access to personal information for financial gain. The new 'work from anywhere world' puts everyone at risk to cyber attacks, especially because threats are harder to track over home networks. The blurred lines between home and work create security nightmares if safety protocols are ignored, or don't exist. One commonly used tactic is phishing.

Phishing messages are crafted to deliver a sense of urgency or fear with the end goal of capturing a person's sensitive data. If your employees fall prey to phishing scams while working from home, it can affect your company network by transferring malware and viruses over internet connections. One phishing email has the power to cause downtime for your entire business and unfortunately the scams are getting more sophisticated on a daily basis, thus harder to detect.

Here are five different types of phishing attacks to avoid:

1. Spear Phishing
Attackers pass themselves off as someone the target knows well or an organization that they're familiar with to gain access to compromising information (e.g., credentials or financial information),

Continued on page 2

Continued from page 1

which is used to exploit the victim.

2. Whaling

Whaling is a form of spear phishing with a focus on a high-value target, typically a senior employee within an organization, to boost credibility. This approach also targets other high-level employees within an organization as the potential victims and includes an attempt to gain access to company platforms or financial information.

3. Mass Campaigns

Mass phishing campaigns cast a wider net. Emails are sent to the masses from a knock-off corporate entity insisting a password needs to be updated or credit card information is outdated.

4. Ambulance Chasing Phishing

Attackers use a current crisis to drive urgency for victims to take action that will lead to compromising data or information. For example, targets may receive a fraudulent email encouraging them to donate to relief funds for recent natural disasters or the COVID-19 global pandemic. According to Google, it has been reported that cybercriminals have sent an estimated 18 million hoax emails about COVID-19 to gmail users every day.

5. Pretexting

Pretexting involves an attacker doing something via a non-email channel (e.g., voicemail) to set an expectation that they'll be sending something seemingly legitimate in the near future only to send an email that contains malicious links.

What to do if you think you've received a phishing email?

First, to help identify it as a phishing email, check to see if the signed-by field was generated by a DomainKeys Identified Mail (DKIM) or a service. DKIM is a good first step in email authentication and is a technical solution to prove that an email is not fake.

For example, if you received an email from name@technology.com, you would see a DKIM in the signature that looks like this: technology-com.20150623.gappssmtp.com. This is how all emails through a domain are processed.

Emails shared through a service (e.g., Drive, Calendar, Dropbox, Box, etc.) do not have a DKIM. Instead, you would see the signature of the provided service (i.e., signed-by dropbox.com).

If you receive a file, and it is not signed by google.com, gmail.com, dropbox.com, it is likely phishing - delete it immediately. It's important to remain vigilant and proceed with caution in these circumstances. Be careful!

Phishing scammers are impersonating file sync and share platforms and sharing fake documents or folders in an attempt to infect your computer.

Good News! **Say Hello To Our New Project Manager, Tammy!**

Tammy Manoharan is the newest member of the Idealogical family. Her software engineering background and her project management experience, and her zest makes her the perfect fit for the role.

She has a sound understanding of the big picture of technology. She takes pride in completing projects on time and on budget.

Join us in welcoming Tammy to her new journey. You can contact Tammy at tammym@idealogical.com

VMware Global Incident Response Threat Report Declares Surge in Sophisticated Cyberattacks

October 2020, VMware released its sixth Global Incident Response Threat Report – "The Cybersecurity Tipping Point: Election, COVID-19 Create Perfect Storm for Increasingly Sophisticated Cyberattacks."

It was discovered that the rapid shift to the remote work environment combined with the accelerated power of the dark web had fueled the expansions of the eCrime groups.

The report revealed that the global pandemic's cybersecurity challenges are now colliding with the 2020 U.S. elections resulting in a surge in cyberattacks. This report is based on an online survey of eighty-three incident response and cybersecurity professionals worldwide in September 2020.

The key findings of the survey are:

1. Incidents of the counter (incident response) IR are at an all-time high, occurring in 82% of IR engagements – suggesting the prevalence of increasingly sophisticated, often nation-state attackers, who have the resources and cyber-savvy to colonize victims' networks. Destructive attacks, which are often the final stage of counter IR, have also surged, with respondents estimating victims' experience 54% of the time.

2. 55% of cyberattacks target the victim's digital infrastructure for the purpose of island hopping. The pandemic has left organizations increasingly vulnerable to such attacks as their employees to shift to remote work – and less secure home networks and devices.

3. Custom malware is now being used in 50% of the attacks reported by respondents. This demonstrates the dark web-scale, where such malware and malware services can be purchased to empower traditional criminals, spies and terrorists, many of whom do not have the sophisticated resources to execute these attacks.

4. As we approach the U.S. presidential election, cybersecurity remains a top concern, and nation-state attackers pose a significant threat. Drawing upon their security expertise – and in line with recent advisories from Cybersecurity & Infrastructure Security Agency (CISA), 1 – 73% of respondents believe there will be a foreign influence on the 2020 U.S. presidential election, and 60% believe a cyberattack will influence it.

The disruption caused by Covid-19 in the form of a rapid shift to the remote work environment has resulted in presenting a massive opportunity for these eCrime groups to restructure their 'for profit' business models. Besides, the power and scale of the dark web have accelerated the expansion of these eCrime groups.

If you have questions or concerns about your business security, email us at info@idealogical.com to address your distress.

Source: www.vmware.com

2 Ways You Can Use Data To Improve Your Business

Do you make data-driven decisions? A survey by Mention, a social media and brand monitoring company, showed that less than 15% of businesses rely on data for day-to-day operations. The reason is that many businesses don't know how to use it. Here's how to fix that:

Organize your data. You need metrics on customers, sales, website hits, phone calls received, etc. If you're using point-of-sale or customer relationship management software, you may have access to large amounts of data. Catalogue and categorize your data – don't just let it collect without doing anything about it. Organized data is useful data.

Collaborate with your team. When you have access to numbers and stats, work with your team to analyze and document. You may need to invest in training to make sure your team is up to speed on how to access and use the data. When everyone is on the same page, you can get the most out of the data you've collected – and start to make data-driven decisions.

Small Business Trends, April 17, 2020

What are eCrime Groups?

Electronic crime, also known as ecrime or cybercrime, refers to criminal activity that involves the internet, a computer or other electronic devices. Many organized criminal groups are involved in criminal activities on the internet.

These groups have moved on from being just hackers who are trying to gain access to computers. eCrime groups are now focusing on low risk and high reward cybercrime activities.

Some eCrime group relates specifically to computers, such as distributing damaging electronic viruses or launching a denial-of-service attack which causes a computer system to deny service to any authorized user.

Top Ways To Protect Your Remote Employees From Cyberthreats

Allowing employees to work remotely comes with its share of benefits, like increased productivity and employee happiness. But it comes with challenges as well, including staying ahead of cyberthreats. Here are three ways to protect remote employees who work from laptops, tablets and smartphones.

1. Avoid unsecured public WiFi. It may be convenient, but cybercriminals can use unsecured networks to steal data. Instead, remote workers should utilize a virtual private network (VPN). Personal hotspots are another option.

3. Develop 'cyber security best practices' for your business. Everyone, including remote workers, should be on the same page when it comes to cyber security. Make sure your employees know the threats and how to stay vigilant online. *Inc., Feb. 12, 2019*

Superstar Of The Month - Ria Latchman

As a part of our company culture, the entire Idealogical team meets once a week on the same day at the same time. Apart from discussing our work week, we praise our teammates for their exceptional contribution towards that week. The person who gets the highest praises the previous month becomes the Superstar Of The Month.

Ria is our first ever Superstar of the Month.

Ria says, "Not many people can say they wake up wanting to go to work, but I do. I am filled with gratitude to be able to work with amazing co-workers and supportive leaders who inspire me to grow and improve in every way possible."