precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume 8: Issue No.2 April 2022

With cyberthreats continuing to rise, we're here to issue a few reminders to help keep you and your team aware.

Dr. Ronald Walcott
Managing Director

Portable storage has become an integral part of the home and office. This enables users to share data between devices and users. While these devices may not be intended to cause harm when shared, in some instances, hackers have been known to intentionally leave devices containing malware to be picked up. Users which find these devices try to access the media and become unknowingly infected and hacked.

"Researchers dropped nearly 300 USB sticks on the University of Illinois Urbana-Champaign campus. 98% of these drives were picked up! In addition, 45% of these drives were not only picked up, but individuals clicked on the files they found inside"

Users should know how to use these devices safely and responsibly both at work and at home. Using removable media within any environment adds convenience, but with all technology, it adds potential risk.

Common examples of removable media

- USB flash drives
- SD cards
- Mobile phones
- CDs

PASSWORDS AND AUTHENTICATION

As we spoke about before, we continue to reiterate that password security is very simple and often overlooked. From commonly used words to recycling passwords on various sites and services, these make it easier for hackers to obtain not just one, but several user accounts that may be tied to an individual email address.

Passwords should be randomly generated and used in conjunction with multi-factor authentication to provide extra layers of security to protect account integrity.

PHYSICAL SECURITY

Many people use books or sticky notes on their desk at home or work. While many attacks happen through digital mediums, keeping sensitive physical documents secured is vital to any security system. If you're having trouble remember-

In this Issue:

ing your passwords, we suggest using a password manager.

Awareness around the risks of leaving your documents and computer or passwords unattended can reduce risk. A clean desk policy at the end of the workday or sessions can help reduce the threat or stolen or copied data and passwords.

PUBLIC WI-FI CONNECTIONS

With remote work on the rise, some employees may utilize public Wi-Fi services to complete work tasks. Public Wi-Fi is naturally less secure as it's open to everyone within range. Some hackers may use this knowledge to "duplicate" a public connection and essentially log all your activity on the connection. Unless absolutely necessary, public wireless connections should be avoided when working with sensitive information. If the connection is necessary, the use of a VPN should be used an enabled to enable a layer of security.

INTERNET AND EMAIL USE

Some employees may already be victims of a data breach by recycling emails for multiple accounts. One study shows that 59% of end users utilize the same password for every account they own. If a hacker obtains the password for any one of those accounts, all accounts are compromised. Within recent years, many large websites have had data breaches and any user who may have had information on those websites may be victims of a leak.

Frequently Asked Questions:

HOW STRONG SHOULD MY PASSWORD BE?

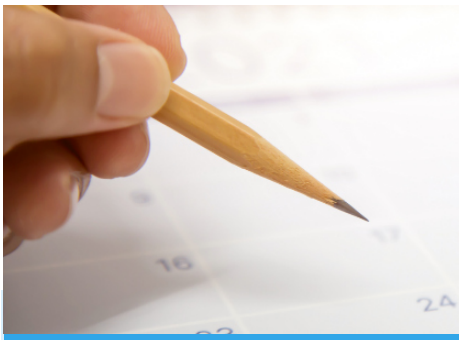
Choose at least 10 characters, from the following character types:

1. Letters (upper & lower case)
2. Numbers
3. Symbols found on your keyboard, such as ! * – () : | / ? ...including blank spaces.

HOW OFTEN SHOULD I CHANGE MY PASSWORD?

Some recommendations suggest changing your password every month, but not only is that a lot to keep up with, it can actually INCREASE your security risks because eventually, you'll end up using a word or phrase that's easy to hack. You'll want to change your password no more than once a year unless there has been a breach.

Businesses usually have a more strict policy in place which enforces password changes every couple of months.



Upcoming Events

VIRTUAL INDIA & SAARC SUMMIT
May 17, 2022

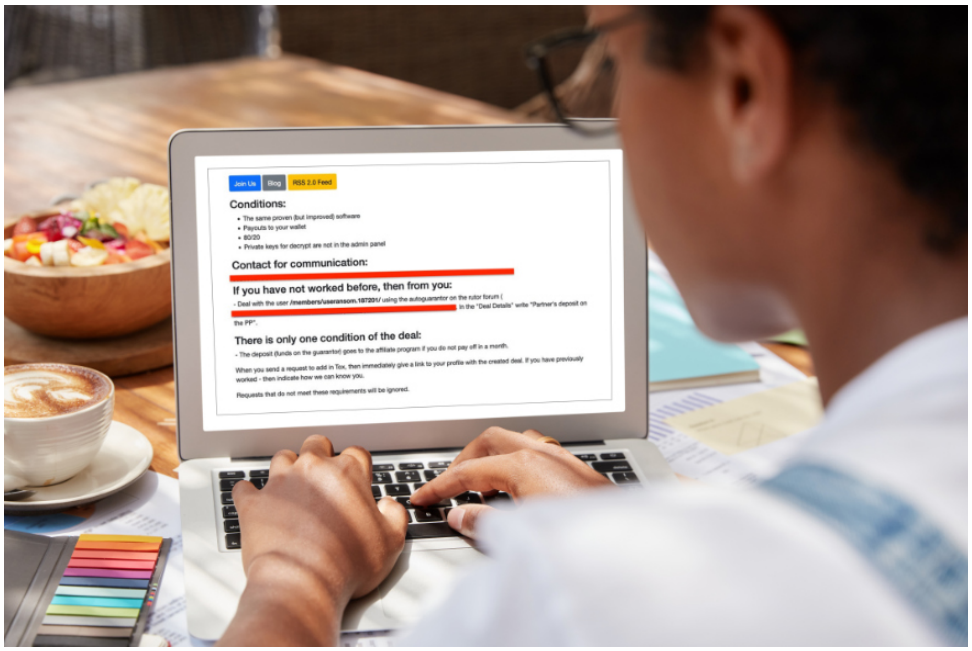
UKI CYBERSECURITY SUMMIT
MAY 24, 2022

FRAUD SUMMIT
JUNE 16, 2022

868-610-7237
salesinfo@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad

HEADLINE NEWS:

Who's Behind Attempt to Reboot REvil Ransomware Operation?



Has the notorious REvil, aka Sodinokibi, ransomware operation come back? Researchers suspect former developers may have restarted the server and data leak site. On Wednesday, the original Happy Blog leak site began redirecting to the new blog, which lists both old and seemingly new victims, including Oil India Limited.

Also on Wednesday, multiple cybersecurity researchers on Twitter attributed a recent ransomware attack at Oil India Limited to either REvil or imposters using the gang's name.

Earlier this month, at the government-owned Oil India Limited's registered headquarters in Duliajan in Assam's Dibrugarh district, a cyberattack was reported, which led to the company shutting down all its computers and IT systems.

A spokesperson for Oil India Limited, a state-owned enterprise of the Government of India under the administrative control of the Ministry of Petroleum and Natural Gas, was not available to comment.

REVIL IS BACK

Soufiane Tahiri, a France-based independent cybersecurity researcher, tells Information Security Media Group that after his initial tweets about the REvil activities, the situation evolved and more hints began to point toward the attackers being REvil itself and not a spoof.

"The very first thing that made me and some other analysts think it's a group impersonating REvil is the fact that the REvil members have been dismantled recently; their blog went off and we didn't hear from them since then," Tahiri says (see: REvil's Infrastructure Goes Offline).

An unnamed source at Oil India shared a screenshot with Tahiri from an infected device that had the exact same ransom note as the one used historically by the notorious REvil group.

In addition, the file extensions of encrypted files are random, like those used by REvil, which also made the source think the attacker was a copycat group, Tahiri says.

REVIL BLOG RESURFACES

Tahiri says he considered it possible that the hackers had obtained REvil code and given it a slight tweak, "until yesterday [April 20], when the original blog of REvil started to redirect to the new one. This means at least one thing: Someone has access to the original server, and this same one is the one behind the attacks, with absolutely no doubt."

Tahiri describes himself as one of "a few threat hunters who think that the main former developer is trying to revive REvil with new members." He says this is still speculation and as far as he knows, someone might be using the same REvil ransom note, extension scheme, and look and feel of the previous REvil Happy Blog. But most importantly, he says, this person has access to the actual old REvil server which, as of Wednesday, has started to redirect to the new blog.

SOURCE:www.databreachtoday.com