KRATIKAL
SECURE FOR SURE

CYBER TIMES

Newsletter by Kratikal Tech

COVID-19 Impact: Stay Cybersecure While Working From Home!

Work from home or not, cyber criminals seem to show no mercy in their persistent attempts of cyber scams!

What is Happening?

Amidst the global crisis of Coronavirus (COVID-19) pandemic, every organization has provided its employees with the facility of WFH (work from home). But outside the secure IT infrastructure of the organization, how vulnerable are employees to cyber threats?

As per the recent cybersecurity investigations, here are the current cyber scams discovered:

Cybercriminals are selling malicious versions of the famous interactive map of COVID-19 cases around the world.

The malicious versions of the legitimate map include stealer malware that steals information from the victim's computer system.

On the other hand, a new malicious domain has been discovered, **coronavirusapp[.]site** that offers to download the Android app for tracking updates on the virus.

However, the malicious application holds ransomware named **CovidLock** which changes the password used for locking the device, thus denying victims from accessing their phones.

This ransomware demands victims $100 in Bitcoin and if the victim fails to pay the ransom, the malware would erase the entire data of the device.

Apart from malicious software, hackers are using phishing emails for fraud activities in the name of Coronavirus and are creating panic amongst victims with extortion emails.

Cybersecurity Tips on Work From Home

Let us not stay naive to the malicious intents of cybercriminals and follow these guidelines in staying aware and alert:

- Make sure that your network access is secure
- Update all the security patches on your work's device
- Use strong passwords in all devices and applications
- Stay extra vigilant about phishing emails and websites
- Beware of online requests asking for personal information
- Follow the security admin's practices for the WFH policy

Learn More About Cybersecurity Solutions

KRATIKAL
SECURE FOR SURE

Spear Phishing attack on rise

Twitter ill-equipped to handle unprecedented hack

What happened?

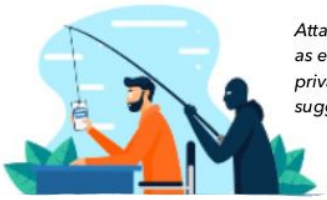
Earlier this month, hackers managed to tweet from more than 40 accounts and hijacked some of the influencial accounts including, Joe Biden, Bill Gates, Elon Musk. The Cyber Criminals were able to share a scam asking for bitcoin.

The hack was widespread and caught Twitter flat-foot. The company's shares were down about 3% after the attack.

How did it happen?

It is said that the hackers succesfully targeted employees who had access to the internal system and tricked them to provide their login credentials. Twitter refered to the incident as "Social engineering".

Others reports suggest that there was an internal level of coordination between the hackers and employees of the company, who were payed to change the email accounts and turning off security features on high profile accounts.



Attackers also downloaded the personal data of as many as eight users- which could include phone number and private messages. None of the accounts were verified, suggesting, people affected were not high profile users.

Prevention for future

Risk based authentication system

Employees who have administrative level control access should be highly educated with proper training, and limited athourity to the influencial accounts.

Use Multi-Factor Authentication

Multi-Factor authentication is a service that adds additional layers of security to the standard password method of online identification.

Watch out for Phishing

Hackers will always try to access private information using tweets, emails & direct messages on Twitter. Being cautious about these phishing mails is very important.

Anonymous sender ID

Always cross check the sender ID before taking any action on the recieved mail.

Mails with attractive offers

Beware of fake mails will offer validity or that offers anonymous rewards.

Unsecure Hyperlink

Cross check if you have been redirect to the link that is secure (https), or to an unsecure hyperlink (http)

Different URL

Hackers tend to create very similar site url to the original one. Therefore it is very important to carefully check the site url.

Minor spelling errors

Lookout for any spelling errors as well as logo for any non-identical mail.

Identity theft

Fake mails tend to ask for your credentials to conduct data theft.

KRATIKAL
SECURE FOR SURE

BEC AND VISHING ATTACKS: SILENTLY GROWING AND VICIOUS FORMS OF PHISHING

HAVE YOU BEEN VISHED?

Vishing or Voice Phishing is a form of Phishing attack where an attacker manipulates the victim to access his personal and confidential information over a phone call.

How does Vishing take place?

Target Hunting
- *Attackers do research on target & perform a thorough background check.*

Luring the Target
- *Attacker calls & uses social engineering tactics to convince victims in providing sensitive information.*

Misusing the information
- *The attacker now misuses this information for further attacks.*

How can you protect yourself against Call Spoofing?

- Block unwanted spam calls
- Don't entertain strangers
- Never share sensitive or your personal information over call
- Avoid IVR calls

AN OVERALL PROTECTION AGAINST BEC ATTACKS

Business Email Compromise (BEC) is a form of phishing attack where cyber criminals spoof email addresses of an organization's executives to victimize employees as well as partners within an organization.

BEC at a glance:

- **BEC has increased by more than 136% in the last two years.**
- **78,617 BEC Frauds have been reported from more than 150 companies.**
- **FBI has reported $12.5 billion loss globally due to BEC attacks.**
- **Fraudulent money transfers sent to 115 countries.**

What can be done?

- SPF — SPF records detect spammers and prevent them from sending messages with forged sender addresses on your domain.
- DKIM — Through DKIM, recipients can retrieve public key from DNS records and use it for decrypting email message headers thus, ensuring that the message is coming from your domain and has not been tampered.
- DMARC policies help in email authentication which will block malicious emails from entering the inbox.

"Remember to protect personal information.The identity saved could be your own."

QUICK TIPS

"AVOID PHISHING ATTACKS"

VALIDATE THE URL

FOR THE WEBSITES YOU ACCESS BEFORE PROVIDING YOUR **PERSONAL DATA**

Powered by

KRATIKAL

SECURE FOR SURE

QUICK TIPS

KEEP YOUR INBOX SAFE

- Verify the Sender ID for authenticity
- Check for grammatical errors
- Hover on links present within the email to confirm the actual URL
- Think twice before responding to emails that sound urgent in nature
- Confirm if the URL/Website is secure over HTTPS
- Be very careful while submitting your credentials online

Powered by KRATIKAL
SECURE FOR SURE

MY p@$$VV0rol IS CREATIVE AND UNIQUE

IT MIXES :

uPpEr & loWer case, L3++3r$, Num&3r$ & $ym&O!$

****

Powered by

KRATIKAL
SECURE FOR SURE