REVALSYS
CREATING POSSIBILITIES

SOCIAL MEDIA CYBERSECURITY THREATS

YOUR BUSINESS NEEDS TO BE AWARE OF

Article from Revalsys Technologies

This article explains about the social media cybersecurity threats a business needs to be aware of

The internet made the world a small place, and social media made it even smaller. But on the other hand, the more “connected” you are on social media, the more exposed you are to the public and, in turn, to cyber-attacks. Social media sites have become a preferred platform for cybercriminals to spread spam and threats, especially due to the increased usage of these sites after the worldwide coronavirus lockdowns.

However, it is not feasible for businesses to avoid using social media. They must meet their customers where they are in order to be relevant and successful. It is important that businesses understand the social media cybersecurity threats they can potentially face and prevent them effectively. Here we have listed some of the most common threats that your business should be aware of:

Phishing

Phishing makes up for most of the social media cyber-attacks. Hackers create fake customer service accounts of your organisation on social media sites and collect personal details or payment information of your employees and customers by sending them malicious links. Phishing can cause financial as well as reputational damage to your organisation.

Human Error

According to researches another major reason for social media cybersecurity attacks is human error. People today share everything about their personal and professional lives on social media sites. They sometimes end up revealing sensitive information about their company in their posts, open a spam link, or download a file with a virus. These acts can open up your business to hackers who can then steal your confidential information to damage your reputation.

Social Engineering

Social engineering is similar to phishing attacks. Here, fraudsters steal social media user data and use modes of personal communication like phone calls, messages, and emails to contact their victims. They pose as reputed companies to dupe users into sharing payment information or transferring money. Fraudsters manipulate their victims by instilling fear in them or creating a sense of urgency, curiosity, excitement, etc., or by falsely gaining their trust.

2020 - Revalsys Technologies. All rights reserved

Account Takeover

Account takeover is where fraudsters gain control of user accounts by stealing their usernames and passwords. Fraudsters then send malicious links to followers of these accounts through private messages, which their victims end up falling for as they trust the accounts they follow. Intentions behind account takeover can be to damage the reputation of a brand, extort money from its social media followers, collect usernames and passwords to misuse them, etc. Most social media users use the same set of credentials for multiple accounts, which makes it easy for fraudsters to steal them.

Ransomware

In a ransomware attack, as the name suggests, a hacker hacks into a social media account and holds its data “hostage”. The hacker blocks the account owner’s access to its data by encrypting it until the latter pays the former a certain amount of money. You must maintain backups of your social media data to be able to recover it immediately after the attack, in the absence of which the only way you can get access back to your data is by paying the hackers ransom.

Connected Apps

Offering social media users the option to lock their accounts does not guarantee them security. You must watch out for connected third-party apps. Connecting these apps with social media accounts gives them access to all aspects of the accounts like their timelines, connections, media, private conversations, etc. Third-party apps are most commonly used by social media account holders to sign into their accounts. This means that one set of credentials can be used by hackers to hack into and steal data of both accounts. Third-party apps may not have the same amount of security as your app, so you must limit the access of these apps to the data on your app. You should only integrate your app with third-party apps that you trust and delete apps that seem suspicious to you.

© 2020 - Revalsys Technologies. All rights reserved.

CONTACTS

For more information on Revalsys Technologies, visit www.revalsys.com

8-2-293/82/1/83-A, 1st Floor,
Road No 12, Banjara Hills,
MLA Colony,
Hyderabad - 500034
Telangana, India

Phone: +91 7032660301

info@revalsys.com