BIZCOMMUNITY

7 tips on mitigating cyber risks to your corporate social media in 2023

By Anna Larkina and Roman Dedenok

19 Jan 2023

Threats to corporate social media are evolving along with perpetrators' social engineering skills at a blistering pace. Sometimes their techniques reach such a high level that even the tech-savvy administrator of a corporate network can't tell the difference between a scam and the truth.

Anna Larkina, web content analysis expert at Kaspersky

Threats to corporate social media are evolving along with perpetrators’ social engineering skills at a blistering pace. Sometimes their techniques reach such a high level that even the tech-savvy administrator of a corporate network can’t tell the difference between a scam and the truth.

As many businesses use social media to promote their products and services, these threats are relevant to an extremely large number of companies. To help them stay safe, Kaspersky experts offer the following advice to mitigate the cyber risks associated with social media in 2023.

7 tips mitigating cyber risks to corporate social media

Here are seven tips that can mitigate cyber risks to your corporate social media:

1. Use caution with direct messages and drafts folder, delete old irrelevant information

Companies should be careful about keeping sensitive information in direct messages – it can pose cyber risks. People often use corporate social media to write directly to brands, asking for help, using the account holder’s product or service. Also, some partnerships, such as those with bloggers, can be negotiated in direct messages.

Sometimes personal or financial information is shared during these conversations, which could remain in the messages folder long after the interaction. If there is a breach allowing cyber criminals to gain unauthorised access to the account, sensitive data may be leaked or used to organise an attack.

To avoid this risk, make it a useful habit to delete irrelevant messages when the dialog is finished and the information it contains is no longer relevant. The same applies to posts – it is worth carefully reviewing what is saved in the drafts folder from time to time.

Roman Dedenok, spam analysis expert at Kaspersky

2. Review old posts to minimise reputational risks

The power of reputation is growing: every word, action, and decision can either help or harm the company's image. Everything published online is of great importance in terms of cyber security as well: when sensitive information (re)appears in public, it almost always ends up hurting a company's reputation and could incur financial losses.

To be on the safe side, spend some time reviewing already published posts, as they might contain information that doesn't fit into the current reality – that might be anything from inappropriate jokes to controversial advertising campaigns. What was normal yesterday, can cause a negative public reaction today.

A review of publications made over the past few years largely reduces related reputational risks.

3. Be careful posting your success stories

Having signed a lucrative contract or reached a deal, we want to post it on social to tell as many people as possible about our success. But we really need to be aware of unwanted cybercriminals' attention. If a potential attacker knows who your suppliers or contractors are, they could try to conduct an attack impersonating them or breaching their accounts and acting on their behalf.

Moreover, the clearer you reflect your company's structure and working methods on social media, the easier it is for perpetrators to organise an attack. For example, if it is possible to trace who is responsible for finance, an attacker can pretend to be this person's supervisor and try to lure them into urgently transferring a large sum of money to a fake account to "close a deal" or "purchase necessary equipment".

Exercising various social engineering techniques, a perpetrator can convincingly impersonate another person, and a victim would hardly notice the fraud.

4 digital advertising mistakes to avoid

JG Bezuidenhout 18 Jan 2023

4. Warn newcomers about risks associated with "new job" posts on social media

After getting a new job, newcomers usually share the news on social, but they do not yet understand how cybersecurity processes are built in this company: for example, how identification works or with whom they can share sensitive information. Therefore, a newcomer is more vulnerable to cyberattacks.

Imagine: a perpetrator tracks this person on social media and collects information about them. Then the criminal writes the new employee a malicious letter on behalf of the company's IT administrator asking to share the password to set up a technical account.

It is highly likely that a newcomer will share the password because they do not know that the administrators would never write such a letter. Moreover, new employees are usually shy, and they might hesitate to ask their colleagues if the letter is authentic.

A tiny little post on social media might turn the employee into an entry point for cybercriminals.To mitigate the risk, offer newcomers a course on information security immediately, and tell them to be extremely careful when posting about a new job.

5. Control account access (and don’t forget to change the password when an employee leaves)

Logins, passwords, and access to the email address used to create a social media account are just as valuable as other internal corporate documents. If an employee who has access to accounts and authentication data leaves the company, it is useful to apply the same rules as when blocking their access to the corporate network.

To begin with, change the password for the email account linked to the corporate social network; then unlink the ex-employee’s mobile phone number and check other authentication methods – for example, a spare mailbox.

6. Do not ignore two-factor authentication

Any account on a social network, not to mention a corporate one, must be securely protected. Two-factor authentication is an absolutely necessary setting for any type of account.The email address linked to the account should be as protected as the social media account itself. Often the attack initially begins with access to e-mail.

After breaching an account, an attacker can configure filters in the mailbox settings to delete all support emails from the social network. Therefore, a user will not be able to restore access to their account, because all emails will be deleted automatically. Not to mention that in a stressful situation we won’t be checking which filters are currently configured in our mailbox.

It is best to register a social media account using a corporate email address. To begin with, it is better protected (assuming the company cares about cybersecurity). Furthermore, in-house security specialists can block access to this mailbox along with all access to the corporate network.

7. Provide your employees with anti-phishing training

To mitigate cyber risks in social media networks, it is not enough to protect your company’s account technically, it is equally important to conduct special training for employees on information security, various types of phishing, and other threats.

According to user statistics on the Kaspersky Gamified Assessment Tool, designed to educate workers and to assist managers in measuring their cyber skills, just 11% of nearly 4,000 employees demonstrated a high level of cybersecurity awareness in 2022, while 28% could not prove sufficient cybersecurity proficiency.Attackers use sophisticated methods of social engineering.

Even the most advanced representatives of Gen Z can succumb to them.The human factor cannot be reduced to zero, but it can be minimised as much as possible with the help of dedicated training.

ABOUT THE AUTHOR

Anna Larkina, web content analysis expert at Kaspersky and Roman Dedenok, spam analysis expert at Kaspersky.