Think before posting anything on social networks, hackers can exploit them to launch attacks

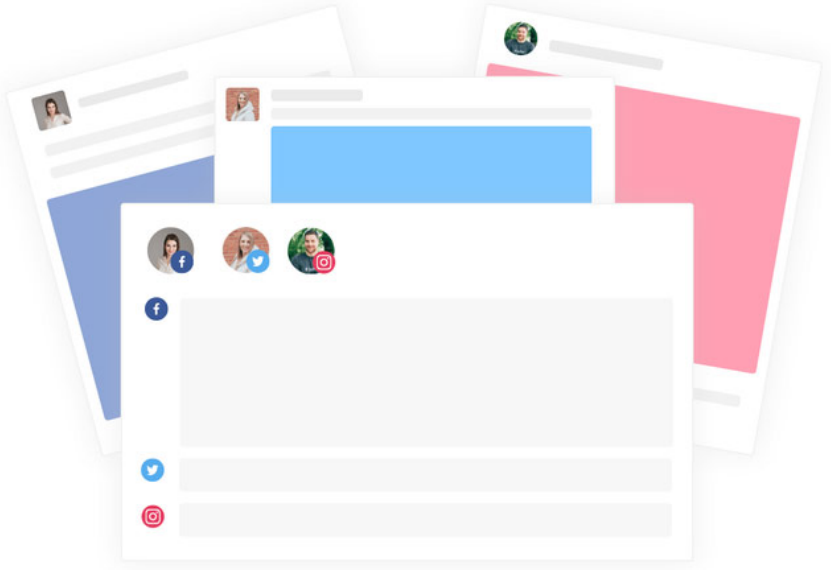
The content you share publicly on social networks can be hacked by people who still walk around the social network to search for photos, videos or anything else that can help them in the vandalism, taking advantage of Turn into an attack tool where you work.

For many people, taking selfies, taking photos at work and sharing on social networks to save happy moments while working is very normal. However, the content you share publicly on social networks can be hacked by people who still walk around the social network to search for photos, videos or anything else that can help them in the vandalism. , taking advantage of turning into an attack tool where you work.

Below is a share of Stephanie Carruthers, a core member of IBM X-Force Red hacker team, an expert in digging up social media posts to find potential security holes, one person redundant ability to view Facebook photos but also hack other people. After reading it, you may have to think a little bit before posting anything on social media.

Carruthers' job is to find security holes of companies before crooks can take advantage of them.

There is a fact that not everyone knows, public postings on seemingly harmless social networks are a true gold mine, containing lots of useful information to help Carruthers' team make attacks. . They can see a lot of things from the background of a photo, such as security cards, laptop screens or even memo sheets of passwords.



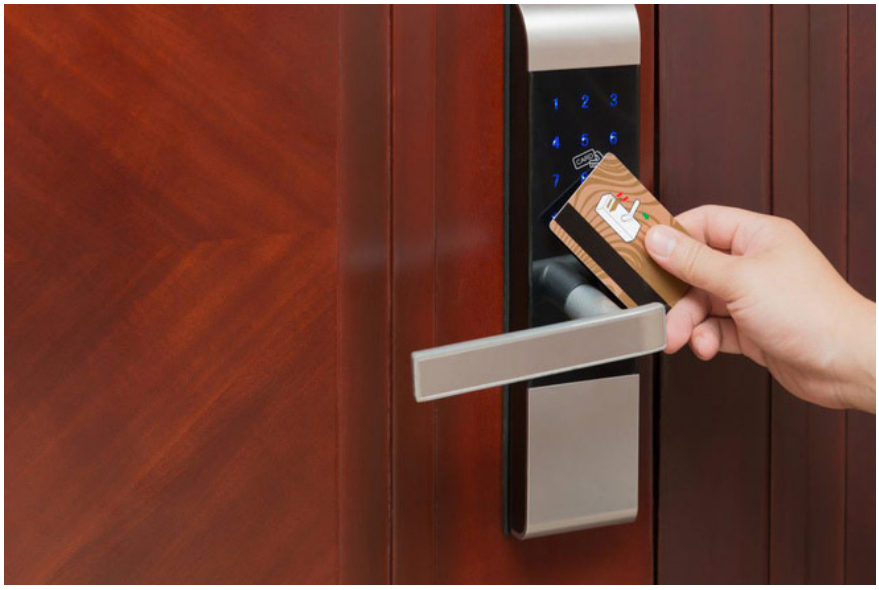
There are 4 types of posts that contain the most risks, which means bringing the most opportunities for hackers.

Collective photos

Collective photos with colleagues at noon or when participating in certain activities together contain more information than you think. Posters showing upcoming teambuilding events, certain meeting schedules or email addresses . are easy to appear in the background of the photo and put you at risk of revealing relevant information.

For example, in the case of a mail leak, the hacker will take advantage of sending you an email containing malicious code that, when opened, will officially turn into a security hole of the company.

The type of card that the company grants to employees



New employees when they receive a new security card or take a close-up card and post it on social networks. This makes Carruthers easily create an identical product with another face in just minutes. Maybe this card doesn't work on scanners but it's enough for Carruthers to get in and out of your company easily.

Job diary video

If the employee did a video about a working day at the company, Carruthers could see the office architecture, the restricted area to go in and the table detailing the future plan . equivalent to Break into the company.

In addition, the laptop screen may display the security software installed. Based on that Carruthers can send to a malicious file device disguised as security software updates.

Complaints or moans

For any company, employees complaining about work, remuneration policies are inevitable. Just knowing that information, Carruthers can compose malicious content, hit right on the psychology of employees.

For example, an employee of a Carruthers company complained on social networks about a little parking space. Taking advantage of this, Carruthers wrote an email describing the new parking policy, along with a false warning that all vehicles outside the parking area would be 'cranked'.

Countless employees received the mail happy to get a place to park and feared that the car would be 'crippled' and immediately clicked on a map of fake parking spaces that was actually a malicious file that Carruthers created, Attached to mail.

After infiltrating into the four office walls, Carruthers could get a lot of information, from sensitive information recorded on meeting room tables and wifi passwords attached to the daylight. Based on that, Carruthers can break the barrier to grasp the company's secrets.

With social media posts, Carruthers may have enough information to look directly into the office without going anywhere.

So before sharing your work-related posts, ask yourself "What is my post that I don't want hackers to know?" ok

1. 4 ways for parents to teach their children to use the Internet and social networks safely
2. What to do to make sensitive photos and videos not exposed and spread on the network?