BIZCOMMUNITY

The scary side of emojis

As emojis are getting more and more popular, scammers, hackers and various shady digital companies are taking advantage of it. If you are obsessed with emojis, you can quickly get into the trap and expose your private data.

It is estimated that every day there are more than five billion emojis shared. As emojis are getting more and more popular, scammers, hackers and various shady digital companies are taking advantage of it. If you are obsessed with emojis, you can quickly get into the trap and expose your private data.

> *"There's one important rule when talking about cybersecurity - never open links, press on ads or download apps or add-ons if you are not sure where those came from. These days you have to check twice, even if we are talking about such a fun thing as emojis," explains Daniel Markuson, a digital privacy expert at NordVPN.*
>
> "One of the growing trends is scams through downloadable emoji keyboards. Be especially cautious of free emoji keyboards, as nothing of value is free".

According to Markuson, if the emoji keyboard is free, it usually means, that the developers behind it rely on a data-driven business model. This means that everything you type on your device, be it a computer or a smartphone, will be continuously tracked and later sold for big money to advertising or other third-party companies. This may seem like not much of a problem, but it becomes an issue if those companies are hacked because of their poor cyber security. Then your personal data might be exposed much more than you would like.

Be careful not only with the usual emojis but with various custom keyboards as well - those allow users not only to add an emoji keyboard but to create personalised avatars as well. Again, if the virtual emoji keyboard is free and you have never heard about its publisher - don't trust it. Better check your official app store and choose something there.

"There are way too many cases when free emoji keyboards spread viruses or other malicious content. So if you would like to use one, at the very least choose one from the official app stores", Markuson suggests. "Viruses and malware usually slow down your computer as they mess around with everything - from pushing ads or phishing sites to hijacking your browser. So if this happens after you install an emoji keyboard - remove it and run a malware scan right away."

Emojis have become bait

And then there is another way how cybercriminals use the cute emotion pictures - emoji malware scam. In recent years, emojis have become their bait of choice, especially when various studies show that emails and newsletters with emojis in the subject line are opened 66% more frequently. If that works for pesky marketers, why not use it for malware scam campaigns?

“Such scammy emails often contain deals that are too good to be true. However, the smiling emoji winking at you at the end of the sentence have a way to convince us that this is a real thing sent by a friendly person,” says Daniel Markuson, NordVPN Digital Privacy Expert. “You open the email, press the link and get that malware into your computer. Those adorable emojis may lead to serious headaches.”

On the final note, most of us chat with friends and send zillions of emojis to kill some time of our daily commute, while waiting for a bus or metro. However, if you or your friends are too much into emojis, you might need a VPN (virtual private network). It will encrypt your internet data and protect your identity and personal information from hackers or identity thieves.