# How Hackers Use Your Stolen Credentials Against You

You might be wondering what happens when all those millions of credentials are stolen and sold on the dark web. Cybercriminals are using the information in various ways. One of them is posing as legitimate colleagues in phishing emails.

In some cases, they send a message with the subject line of “unpaid invoice” or something similar. Attached to the email is a document that includes common malware that will infect your computer and steal your online banking credentials.

To avoid falling victim to this, and similar scams, watch for some of these as red flags:

- Unexpected attachments or links included in the message.
- A supposed invoice is included.
- A dialogue appears asking you to enable macros.
- Information from your social media or networking profile is included in the message.

## 3 Tips to be Better Protected

- Be cautious about the information you post on social media or professional networking sites. This is often used for targeted phishing attacks (spear-phishing) and, in many cases, are so well done that if you are not paying attention, you could fall victim.
- Beware of pop-up or warning fatigue - this happens when a user gets inundated with dialogue messages whenever browsing the web and overlooks them or clicks on them without actually reading them. The hackers count on this happening and will implement malware behind those buttons. If you click the wrong one, you may lose a lot more than patience!
- Never enable macros unless you are 100% certain that it is necessary or that you, or someone you know, created them. Macro malware is on the rise lately and has been seen in a lot of the newly-created versions of malware.

Get the lastest information from our website. Scan the QR Code to go directly to this page.