Think Before you Click

STAYING SAFE ON SOCIAL NETWORKS!

Cybercriminals use everything at their disposal to launch malicious attacks and social networks are heavily leveraged by these bad actors. Social networks are mainly used by cybercriminals to collect information about users to be used for malicious intent.

There are two main strategies that are used to collect this information.

The first strategy is the use of fake websites to steal personal and/or confidential information such as logins and passwords.

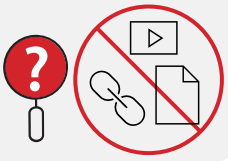
The second strategy is harvesting what seem like unimportant personal details that are shared on social networks but that are used by cybercriminals to launch phishing attacks.

Here are 13 things to remember to stay safe on social networks:

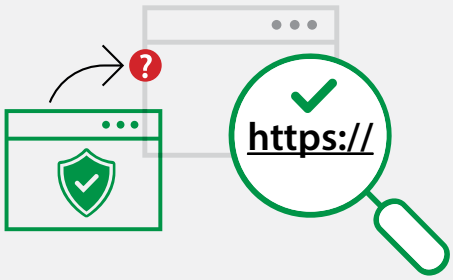
1. Spelling errors are telltale signs of phishing scams. Check that URLs are spelled correctly. Example: Facebook spelled with one “o”

2. Never click on links in suspicious messages sent through direct messages

3. Never click on unverified links, videos, or files



4. When being re-directed to another site from a secure site, verify the address you are being re-directed to see if it is legitimate. In many cases, if you are being re-directed, the site that is re-directing you will tell you that you are being re-directed and why



MicroAge

Here are 13 things to remember to stay safe on social networks:

5 Use reputable security software

6 Limit the information available on your social media profiles e.g. home address

7 Don't save your login information on shared computers

8 If something looks too good to be true, it probably is. Offers for free product or money for example. Don't follow or click on those links

9 Don't accept "friend" requests from people you don't know

10 When asked for information to update your account or to re-enter your login details, verify the URL

11 If you receive an unusual message from someone you know, contact them outside of the social network site to check on the validity of the message

12 Remember: banks and governments never ask for your personal information on social media. Don't be intimidated to respond. Also remember these institutions will never ask such information through email or text either

13 Don't respond to invitations to connect unless you know the person or company