
Bank AL Habib
SOCIAL MEDIA
/BAHLOfficial

SOCIAL MEDIA

Fraudster can analyze your posts and use them to gain access to your personal and organization's information with whom you work with. For instance:

- They can use information you share to guess the answers to the secret questions that reset your online passwords
- Create targeted email attacks against you known as spearfishing
- Call someone in your organization impersonating you
- Attacks can spill into the physical world, such as identifying where you work or live

HOW TO AVOID BEING A VICTIM

Avoid click-baiting – Fraudsters have been known to post links that attract attention; the links, of course, often direct to malicious websites such as giveaways, survey scams etc.

Do not share your personal and confidential information such as phone number, address, bank details, debit/credit card numbers etc. on social media sites. Experienced password hackers or phishing sites can assemble together your shared information to gain access to your account, or use your identity to create a new one

Keep a complex alphanumeric password (e.g. erPxyT@2!), change them regularly and never share with anyone

Be suspicious of unsolicited Email/SMS/Calls, do not respond to them immediately and always verify sender/caller details for authenticity prior responding to any Email/SMS/Calls

Watch out for suspicious messages including messages with urgency, catchy product offer, posts having URL with captivating statements as 'OMG this post of you…' or 'Have you seen this new tech… '

Be careful of what you post online. Anything you post can or will become a public and permanent part of the Internet.