IT Security Awareness: Phishing Avoidance Tips & Measures

BUILDING BONDS

Dear User,

In an effort to enhance our Company's cyber defenses and to create awareness, we want to highlight the basics of phishing that everyone should be aware about.

"Phishing" is the most common type of cyber attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, Personal Contacts, credit card information, bank account details etc.

WHAT YOU SHALL DO!

To avoid phishing schemes, please observe the following best practices:

❑ *Do not click on email links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.*

❑ *Do not provide your sensitive personal information (like usernames & passwords or contact details etc.) over email or Phone call*

❑ *Watch for email senders that use suspicious or misleading domain names.*

❑ *Inspect URLs carefully to make sure they're legitimate and not imposter sites.*

❑ *Do not try to open any shared document that you're not expecting to receive.*

❑ *If you can't identify if an email is legitimate or not, please do not open such email.*

❑ *If you receive an e-mail that you suspect to be a whaling attempt, or if you are unsure of an e-mail's legitimacy, please do not respond or open it. Instead, report the same immediately.*

❑ *Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner.*

❑ *Remember, never reply to anyone's request for personal information, usernames, passwords, Phone Numbers or money via email or Phone Calls.*

❑ *Keep your system updated with latest Antivirus solution.*

IT Security Awareness: Phishing Avoidance Tips & Measures

CAUTIONARY MEASURES

❑ *To exercise caution against fraudsters who may use fake email IDs, fake profiles on Social media (Whatsapp, Facebook etc.,) domains, websites, etc. by impersonating themselves to be from the Company or any A K Group entity and claim to be offering credit facilities at lower rates of interest, collect customer account details, ask for advance money to process credit facilities, etc.*

❑ *We do not call for any advance money to process any credit facility and we have a detailed system in place to verify the loan application in line with regulatory requirements/ guidelines/ directions prior to sanction of any such facility.*

❑ *We never ask fro sensitive information like OTP or PIN for any credit facility related services. You refrain from sharing any OTP/ PIN with any person or authorizing UPI requests in wallets, received from unknown sources, as the same may lead to a fraud, through which, money may be debited from your Bank account and credited to fraudster's account.*

❑ *We have legitimate domain name "akgroup.co.in" and do not use other domain name*

❑ *Before responding to any such email, please contact us to verify the legitimacy of any such communication.*

❑ *Please note that any person responding to any such communication, will be dealing at his/ her own risk and responsibility. The Company and/or any of its Group Company will not be responsible for any loss suffered or otherwise in this respect.*

IT Security Awareness: Phishing Avoidance Tips & Measures

WHOM TO CONTACT

□ In case you encounter any such incidents, which claims to be from A. K. Group - ***Write to us on at itsupport@akgroup.co.in*** with basic details including name, contact details (email Id, address and phone number), details of frauds, documents related to fraud, etc.

□ The incident shall be brought to the notice of the Company within 72 hours.

□ For Financial Cyber Frauds – ***File a complaint to RBI on www.cybercrime.gov.in or through cybercrime helpline number - 1930***

□ Also, you can reach out to the nearest police station and file an FIR.

"Thanks for helping us to keep AK Group network, systems, Data and our people safe from these cyber threats. We are happy to resolve your grievances"

"Awareness" and "Alertness" are the keys to avoid cyber crime