Kogta
FINANCIAL
FREEDOM TO GROW

GLORIOUS
25
YEARS

DO'S AND DONT'S FOR CYBER SECURITY

PASSWORDS

✓ Use Hard to Guess passwords.

✓ Password should have Minimum 10 Characters with Uppercase, Lowercase or Special Character.

✓ Different Passwords for different Accounts.

✓ Keep them confidential.

✗ Don't leave Passwords lying around the office.

✗ Don't post any Passwords on Public Sites.

✗ Don't Share your Passwords with any other Person.

MANAGEMENT OF INFORMATION

✓ Maintain Confidentiality of information.

✓ Lock your System when not in Use.

✓ Be aware of your surroundings when printing, copying, faxing, or discussing sensitive information.

✓ Destroy information Properly when it is no longer needed.

✗ Don't Post any private or sensitive information, such as credit card numbers, or other private information, on public sites, including social media sites.

✗ Don't be tricked into giving away confidential information, it's easy for an unauthorized Person to call and pretend to be an employee.

✗ Don't respond to Phone calls and Mails requesting confidential information.

Kogta FINANCIAL FREEDOM TO GROW

GLORIOUS 25 YEARS

DO’S AND DONT’S FOR CYBER SECURITY

MAILS

- ✓ Always check “From” field to Validate the sender.
- ✓ Always check for files with a Double Extension.
- ✓ Always report suspicious emails to Information Technology support team or engage them for guidance before proceeding.
- ✓ Always look closely at the URL included in the mail.

- ✗ Don’t open any email attachments that end with .exe, .scr, .bat, .com, or other executable files that you do not recognize.
- ✗ Don’t ever click embedded hyperlinks within email messages without first hovering your mouse over them to see where they will take you.
- ✗ Don’t respond or reply to spam in any way.

BE CAREFUL WHAT YOU CLICK

- ✓ Check properly whether the link you are clicking is received by an authorized person or not.
- ✓ Install Security Software in case of clicking mistakenly on wrong link it will protect our system.

- ✗ Avoid visiting unknown websites or downloading software from untrusted sources.
- ✗ If attachments or links in the email are unexpected or suspicious for any reason, don't click on it.

DO'S AND DONT'S FOR CYBER SECURITY

PHISHING ATTACKS

✓	✗
✓ Do check for any type of Grammatical errors and the id of the sender. ✓ Educate your friends and family about such types of errors so that they avoid opening such emails or forwarding them to you without any knowledge.	✗ Don't open Emails from un-known person or sources. ✗ Hover over the links before clicking to figure out where they are direct and if the link seems unsafe, do not click it.

Desktop or Laptop

✓ Use Company allocated Desktop or Laptop for officially works.	✗ Personal devices like Laptop, Tablets are prohibited in office premises.

DO'S AND DONT'S FOR CYBER SECURITY

INSTALL ANTI-VIRUS/ANTI-MALWARE PROTECTION

✓	✗
✓ Do use Windows anti-Virus Protection. ✓ Do adopt Smart Anti-Virus Practices in the workplace.	✗ Don't install just any third-party antivirus program. ✗ Don't forget the firewall Protection.

PUBLIC WIFI

✓	✗
✓ Make sure the Public Wi-Fi you are using has a valid VPN. ✓ Use Mobile Network or any other connection if public Wi-Fi is not having a valid VPN.	✗ Don't use public Wi-Fi if it's not having a valid VPN. ✗ Don't enable your Bluetooth and Wi-Fi on every Public Places you visit.