

自治体の首長、企業の代表等になりすましアカウントに注意!!

自治体の首長、企業の代表等になりすまし、公共施設や団体、議員、企業の社員等に宛てた不審なLINEやメールが急増しています。



パターン① なりすましLINEアカウント

① なりすまし送信者



LINEの友だち申請



代表等になりすましたLINEアカウントから、公開されている関係者の電話番号等を利用して友だち申請をする。

②



LINEグループ

新規プロジェクトの為、口座情報や個人情報を共有してください。

LINEグループに招待し、情報をグループ内に共有させ、盗み取ろうとする。

パターン② なりすましメールアドレス

① なりすまし送信者



新規プロジェクトの為、新しいLINEグループを作成して、二次元コードを送ってください。

② 担当者



LINEグループを作成しました。二次元コードを送ります。

代表等になりすましたメールアドレスから、ホームページ等で公開されているメールアドレス宛にメールを送信。

指示通りにLINEグループを作成し、二次元コードをメールで送信。

③



LINEグループ

グループに他の担当も参加させてください。口座情報や社員の個人情報を送ってください。

代表等になりすました送信者がLINEグループに参加し、他の担当者もグループに参加させて情報を盗み取ろうとする。

LINEグループから盗み取った情報を利用して、詐欺や不正送金、取引先等へのビジネス詐欺メール等の被害発生が考えられます。不審なメッセージには応じず、組織内で情報共有する等注意喚起をお願いします。

