

こうちのまもり

高知県警察本部 サイバー犯罪対策課

⚠ 情報漏洩に便乗したフィッシングに注意 ⚠

『おわび・本人確認・補償』などを装う連絡に注意！

「おわび」、「本人確認」、「補償」などともっともらしい連絡を装い電話・電子メール、SMSにより連絡してくる。

あなたの名前や住所を知られていても相手方が本物とは限りません。

（※フィッシング行為）



言葉巧みに認証コードを聞き出そうとしたり、貼付のURLに誘導させる場合などに注意！

たとえば、『【重要】○○社の個人情報漏洩に関する補償のお知らせ』などとして、

★「おわび金を振り込むのでリンクのURLで手続きしてください」

★「本人確認のため認証コードを教えてください」

など言葉巧みにあなたのお金や重要情報を盗み取ろうとしてくるので注意してください。



※　様々な犯罪被害に発展するおそれがあります！

被害に遭わないために

- ☑ 届いたメールにはられたURLからではなく、公式サイトや公式アプリからアクセスして確認する
- ☑ 多要素認証などは積極的に活用する
- ☑ 使い回しているパスワードがあったら変更する



被害に遭ってしまったら **警察に通報・相談** を！

最寄りの警察署又はサイバー犯罪相談窓口 ➡

https://www.npa.go.jp/bureau/cyber/soudan.html



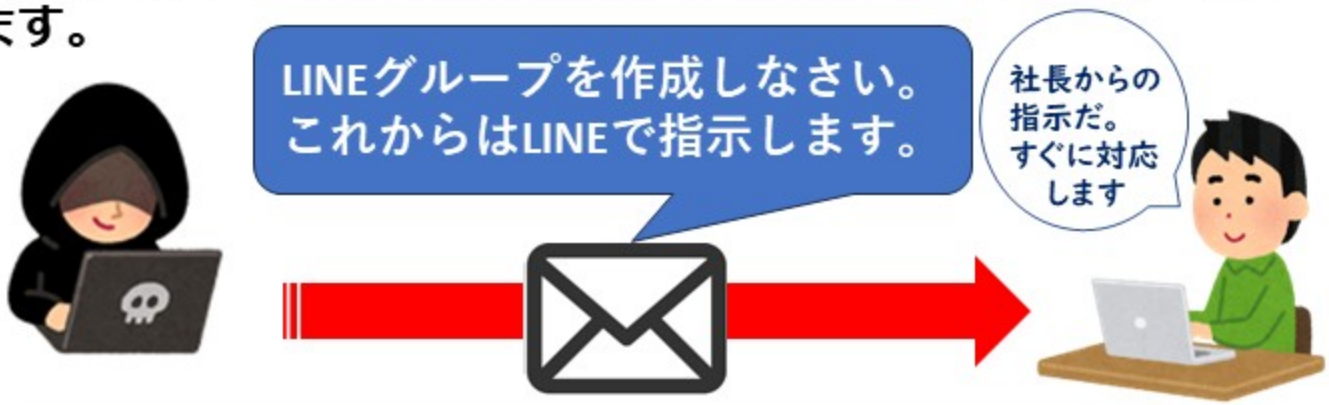
こうちのまもり

高知県警察本部 サイバー犯罪対策課

⚠ ニセ社長・会社役員詐欺に注意 ⚠

差出人を社長名にしたメールを社員や取引先に送る

実在する社長名や会社名などを騙る詐欺メールに関する相談が急増しています。メールには「LINEグループを作成してQRコードを返信して」などと指示してきます。指示に従いQRコードを返信すると、LINE上で社長を騙った犯人から取引を装った振込・送金の指示が行われ、詐欺の被害に遭ってしまいます。



社長からのメールと思い込み、メールの指示通り従ってしまうと・・・

LINEでのやりとりが始まり、**多額の嘘の振込や送金**を指示され、会社のお金が騙し取られることとなる。



被害に遭わないために

- ☑ 不審なメールは無視して削除する。
- ☑ 差出人本人に直接・電話などで確認する。メールに返信で確認しない。
- ☑ 本文のURLにはアクセスしない。添付ファイルは開かない
- ☑ 社内の指示系統に変更や多額の送金などの案件は社内で二重チェックなどの承認フローを構築しておく。