Do you know who you're talking to?

Fraudsters are scamming businesses over the phone

Financial Fraud Action UK
Working together to prevent fraud

CIPFA COUNTER FRAUD CENTRE

Vishing

Telephone fraud is being used increasingly by criminals to deceive businesses into revealing company financial information or to encourage the transfer of funds into a bank account held by the criminal. This type of fraud is known as 'Vishing'.

Posing as a company supplier, a police officer, or a member of staff from a bank or building society, criminals will make an attempt either to obtain your company bank account details or will ask for bank payee details to be altered so that regular payments normally transferred to a genuine supplier account are instead made into a fraudulent account.

Variations on the scam

A variation of the fraud involves the criminal posing as a senior bank official or police officer investigating internal fraud at your company bank. They will attempt to persuade a member of staff that in order to protect your company's fund, all money must be transferred to a 'secure' account. The member of staff will then be talked through an online transfer or be encouraged to contact their local branch to move the fund. They are advised not to give the bank a reason for the transfer in case the teller is involved in the internal fraud.

A further variation involves your company receiving a call from your 'bank' to validate a payment. The caller then obtains details of real payments made, including sort codes, account numbers and monetary amounts. Armed with this information, the caller telephones again later that day advising that these payments have stalled and need to be re-entered online to another account, with details supplied by the caller.

It takes two to terminate a call

A key tactic used sees the criminal, again posing as a legitimate company supplier, encourage a member of staff to double-check the validity of their call by hanging up and calling them straight back. By not terminating the call at his or her end, the criminal keeps the line open, when the member of staff 'calls back' using a valid, on-file number, it is the criminal that they reach. A sophisticated variation of this scam involves the fraudster playing a recording of a dial and ring tone to add legitimacy to the call back.

To prevent Vishing, it is crucial to ensure that, within your company, every member of staff knows who they are talking to.

How to avoid Vishing

Be wary of:

- Unsolicited telephone calls
- Callers who suggest you hang up and call them back
- Callers who advise that your company or organisation's payment has been blocked in the transfer system
- Callers who request that you transfer funds to a new bank account

Remember

- Do not assume that every telephone call is an honest one. Criminals may already have enough information about your company to appear genuine.
- Be wary of requests for financial information and alterations to bank transfers.
- Terminate the conversation if you feel suspicious of the caller.
- Remember that caller display IDs can be manipulated to disguise the origin of the call. If in doubt, call back using an independently verified number.
- Use a different line to validate a call. Be aware that it takes two people to terminate a telephone call. The line can be kept open if the caller does not end the call, meaning that if you do attempt to call back in order to validate them, you will reach the same person.
- Review company policy on what information staff are permitted to provide to a telephone caller.

For further advice and guidance visit www.financialfraudaction.org.uk/vishing

If you think you may be a victim of this type of fraud please contact Action Fraud to report it on 0300 123 2040 or via the website reporting template at www.actionfraud.org.uk

Financial Fraud Action UK
Working together to prevent fraud

CIPFA COUNTER FRAUD CENTRE

@FFA UK Financial Fraud Action UK