

Common Fraud Scams – Increase Your Awareness

Based upon research & reports which were published by the Europol

CCR CHAIKIN COHEN
RUBIN & CO.

“Professionalism of a Big Firm, Personal Attention of a Small Firm”

www.ccr.co.il



Fraud Awareness

Fraud occurs usually by "requesting an urgent business transaction" via email fax or telephone. The sender stresses the urgency, confidentiality and importance of trust and honesty to sway the reader into believing the validity of the request by claiming to be a corporate entity, possibly government or other union.




Fraud Targeting Employees



KEY TARGETS

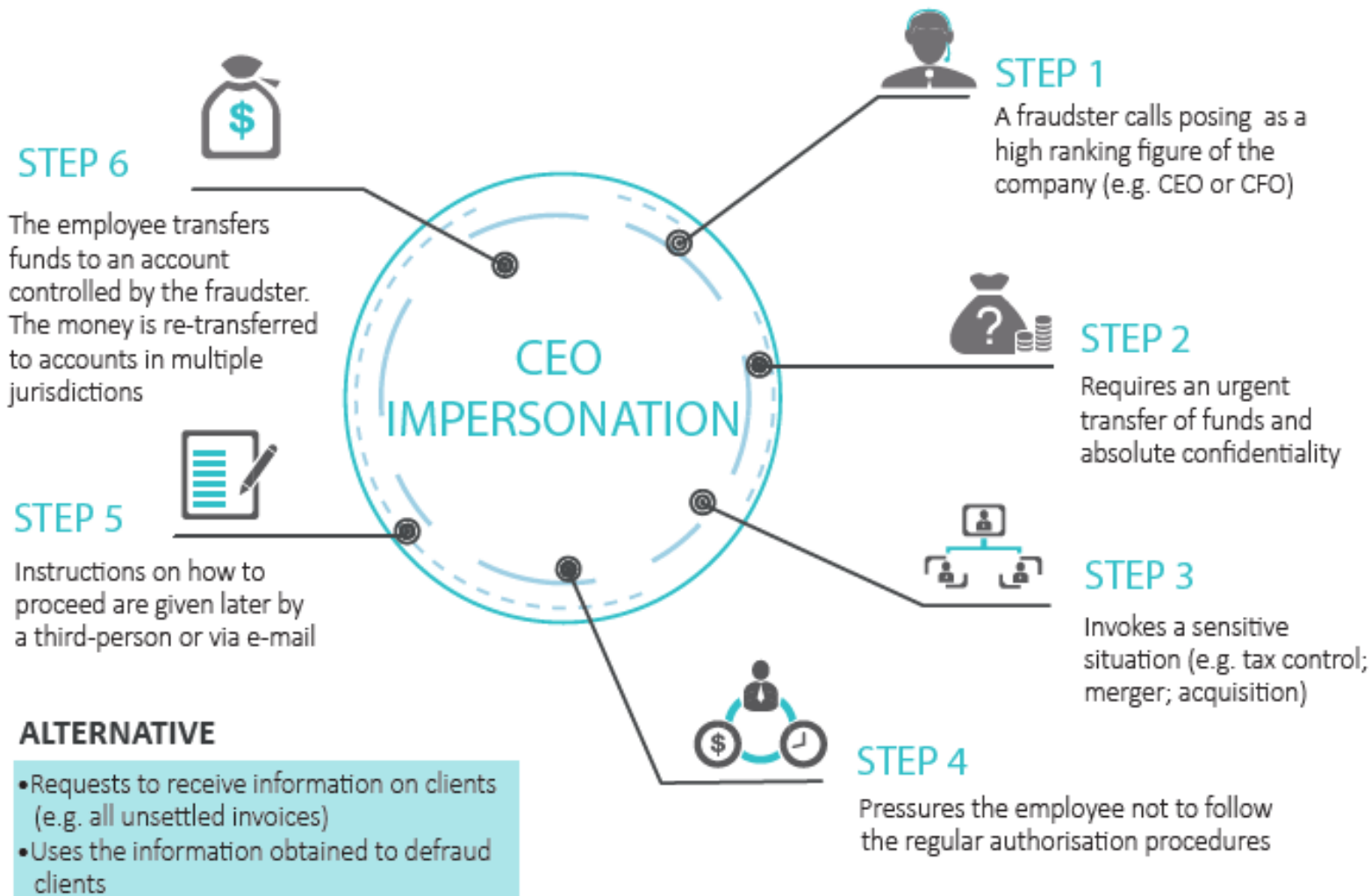
Mid-level employees in
financial or procurement
services



HIGHLY ATTRACTIVE CRIME

large profits and low
risk of detection

Know the Fraud Scams Targeting Employees

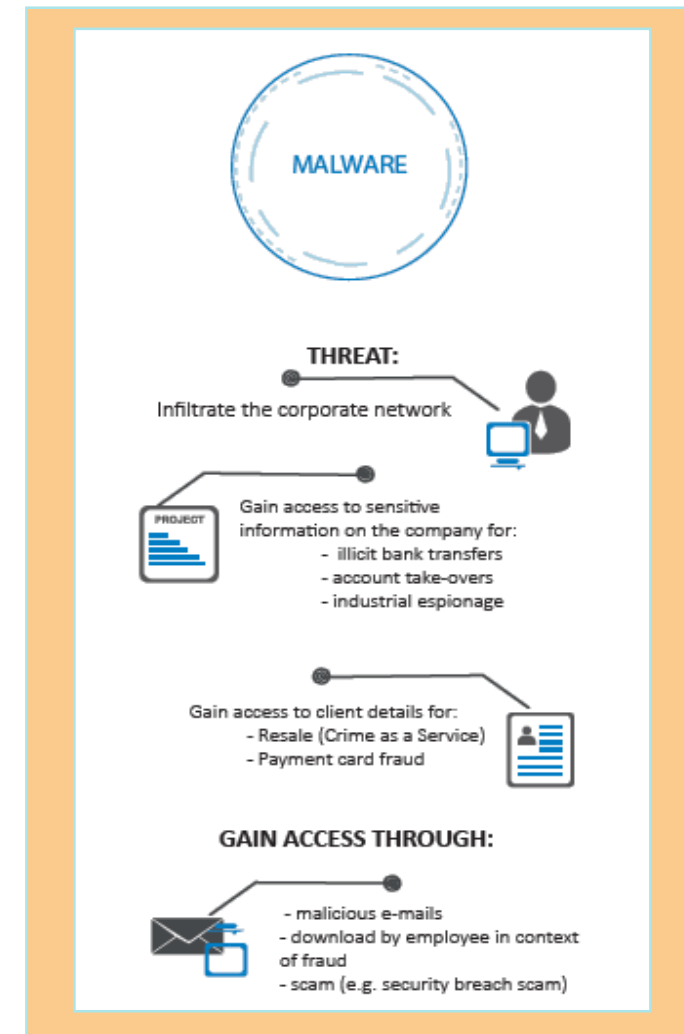
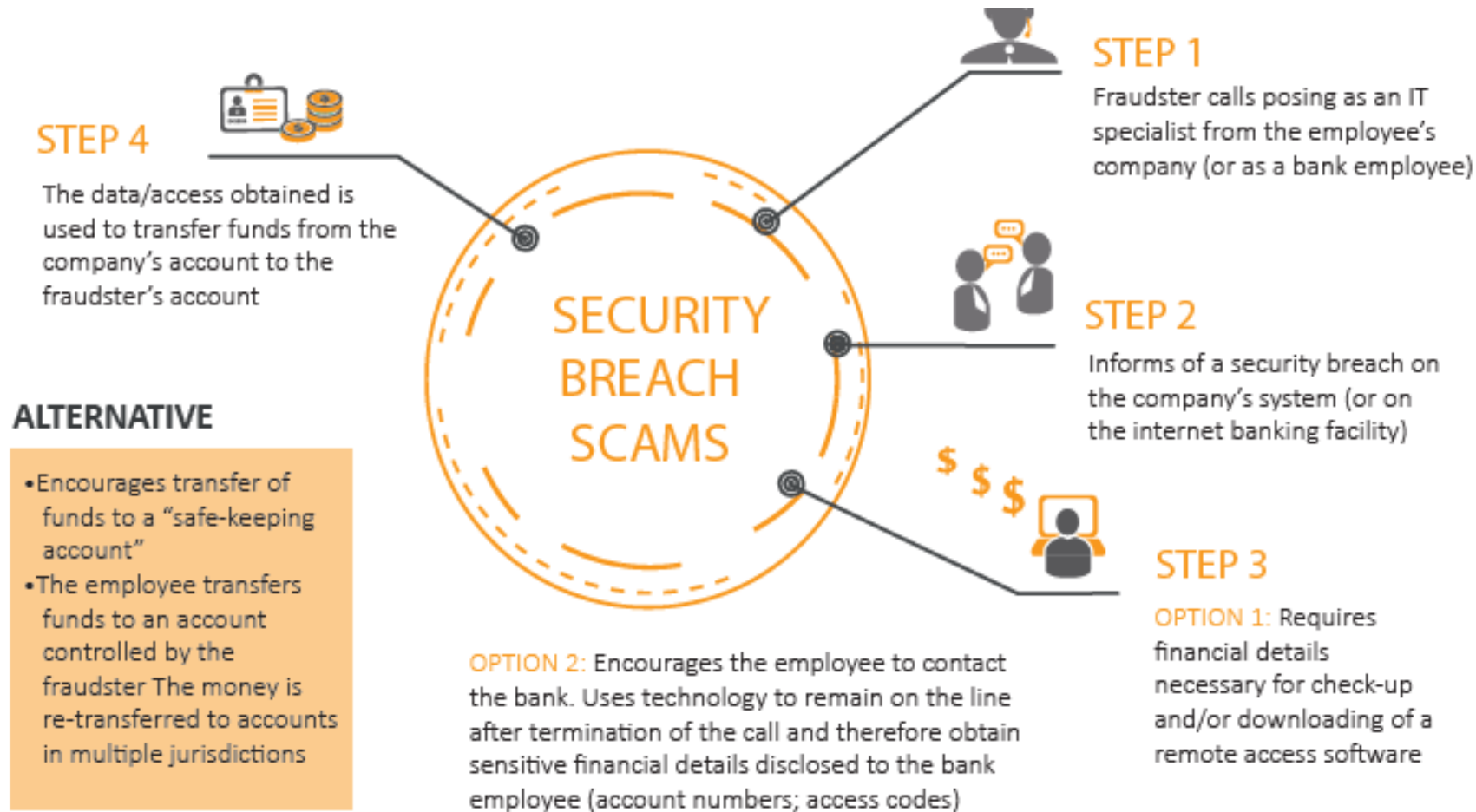


HOW DO FRAUDSTERS CONCEAL THEIR IDENTITY?

- Use forged documents with legitimate company logo/signatures obtained online
- Use copycat e-mail addresses
- Disguise the origin of the call through applications faking the caller's identity (display the number of the service/individual they impersonate)

- ✓ Request for absolute confidentiality.
- ✓ Threats or unusual flattery/promises of reward.

Know the Fraud Scams Targeting Employees



Advised Preventive Precautions

- ✓ Spread awareness of security incidents within your company.
- ✓ Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
- ✓ Avoid sharing sensitive information on the company's hierarchy, security or procedures. Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- ✓ Never open suspicious links or attachments received by e-mail. Be particularly careful when checking your personal mail boxes on the company's computers

Advised Preventive Precautions

- ✓ Always carefully check e-mail addresses when dealing with sensitive information/money transfers. Fraudsters often use copycat e-mails where only one character differs from the original.
- ✓ If you receive a suspicious e-mail or call, always inform your IT department; they are the ones in charge of such issues. They can check the content of suspicious mail and block the sender if necessary.
- ✓ If you receive a call/email alerting you of a security breach, do not provide information right away or proceed with a transfer. Always start by calling the person back using a phone number found in your own records or on the official website of the company; do not use the number provided to you in the mail or by the caller. (fraudsters can remain online after you hang up).

Example Email - IT Update

From: uec_100@hotmail.com **Unknown Email Extension and Non-Professional Subject**
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530



Punctuation Errors

Dear Email User,

This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support on your account and security. If you choose not to update your account on or before **4th February, 2015**, you will not be able to read and send emails, and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

Update Your Account

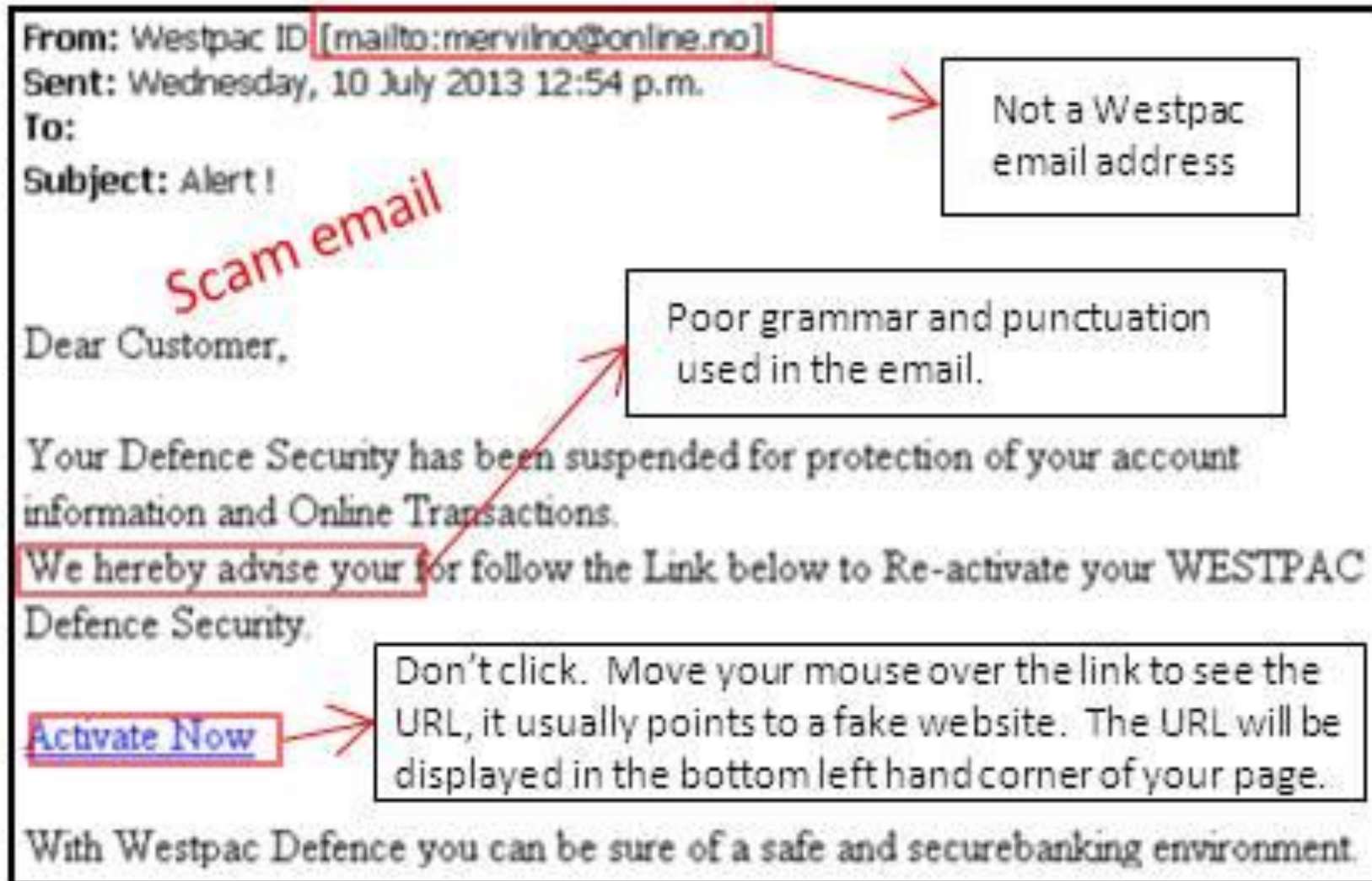
Link to Malware/Virus Page

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.

Thank You

Outlook Warning! Member Service

Example Email – Suspended Account



MALWARE

- Unsolicited e-mails with generic greetings
- Unsolicited e-mail containing suspicious links/URLs

Example Email – Security Alert

Know the Signs

- ✓ Use of particularly alarming tone by an IT/security officer.
- ✓ Request to download external software (e.g. remote access software).
- ✓ Offer of a safe-keeping account.
- ✓ Unsolicited call/e-mail requesting information on internal procedures for payment, procurement or financial information (account numbers, access codes).
- ✓ Feeling of emergency.
- ✓ Pressure.

PayPal™

PayPal Customre Care

Dear Customer, **Grammer & Punctuation**

Hi,

Dear customer

At first Thank you for paying attention to PayPal Customer Care.

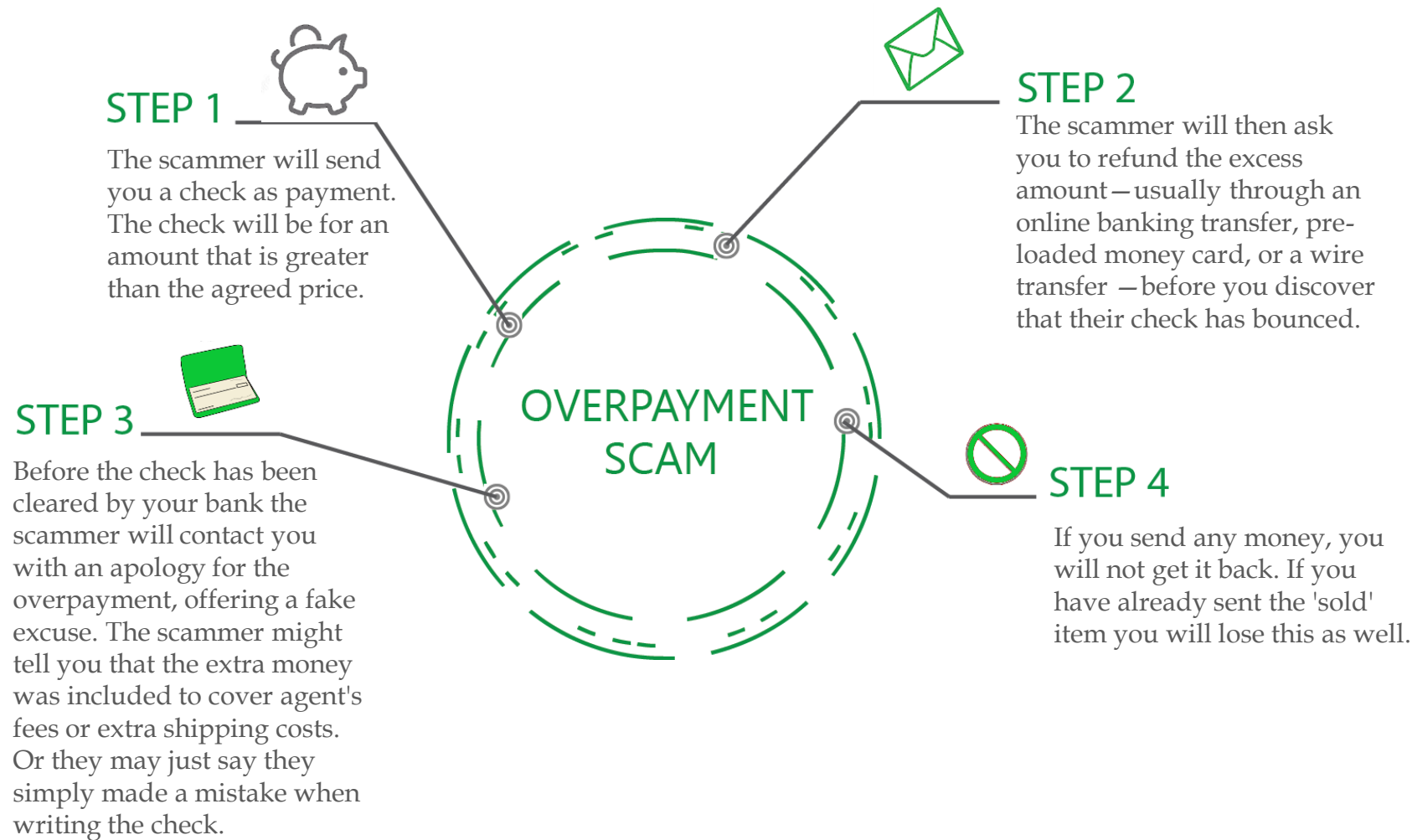
We contact you for confirming you Paypal account.because of security reason you have to confirm you account in PayPal again.our log on your account show us some illegal usage then we want you to pay some time and Confirm your account again. for confirming just login to PayPal with attached form just from your personal computer. pleso do not use public computer.this form is for avoiding others to access your account. by logging on your computer we can keep you secure from man in the middle attack.

we are waiting for your confirmation.

Thank you again for contacting PayPal Customer Care.

Regards,
PayPal Customer Care.
895485654

Know the Fraud Scams Targeting Employees



- ✓ If you have been sent a check for more money than the agreed price, send it back and ask for another check with the correct amount.
- ✓ **Do not** agree to repay the difference until you are certain that the check has cleared.
- ✓ Do not send the items to the buyer until the check has cleared in your bank account.
- ✓ For items of high value, do not allow potential buyers to inspect the goods without someone else being there.

Know the Fraud Scams Targeting Employees

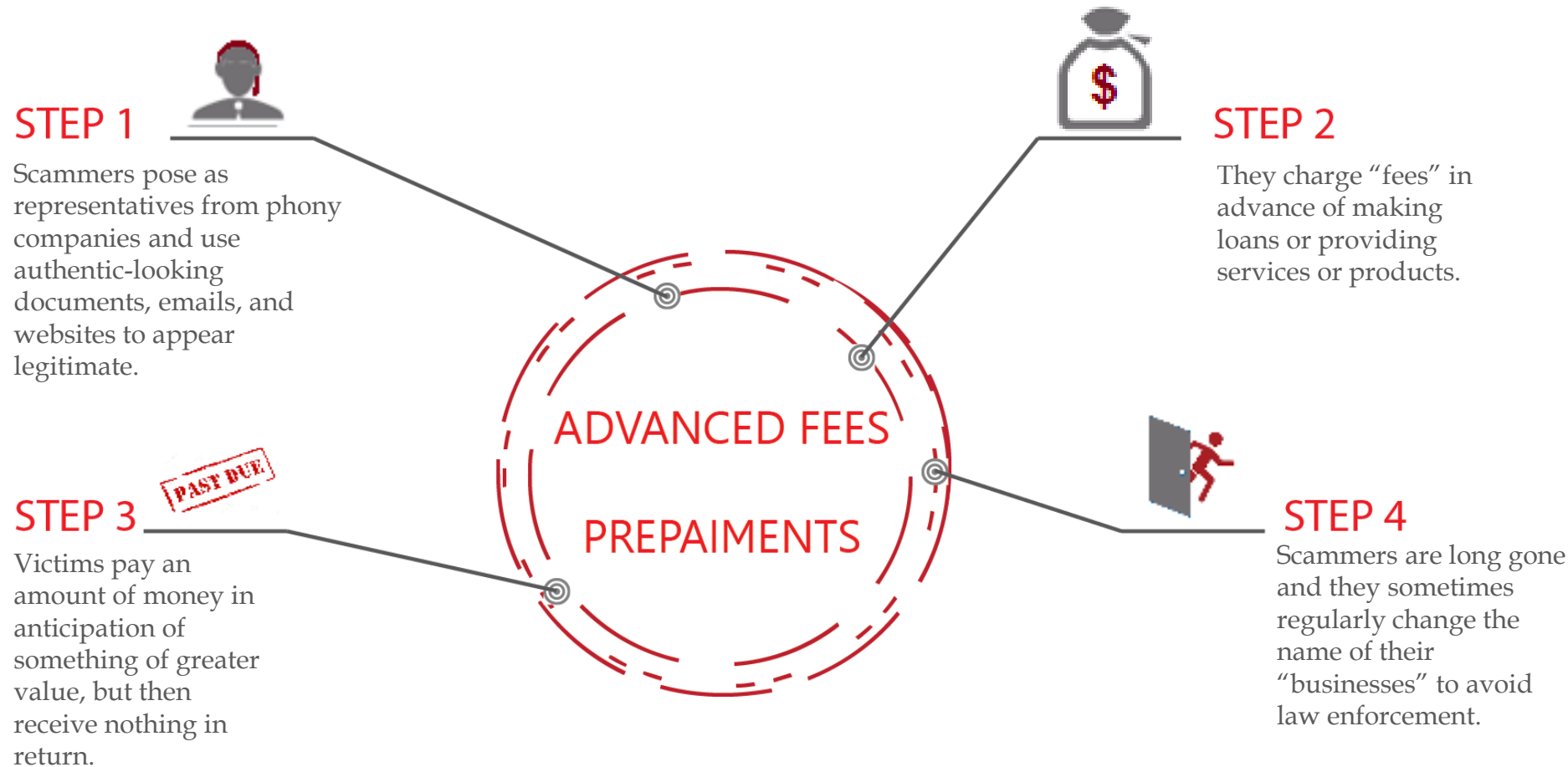
- ✓ Sudden change in contact/payment details of an international supplier (would normally be announced a few weeks/months in advance).
- ✓ Change occurring shortly after a significant order was passed or shortly before a deadline for payment.



Advised Preventive Precautions

- ✓ Consider assigning responsibility to an employee whom others can consult in case of doubt.
- ✓ If a supplier informs you of a change in payment details, always contact them to confirm the new information. Keep in mind that the e-mail/phone number provided on the invoice might have been modified.
- ✓ Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- ✓ In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.

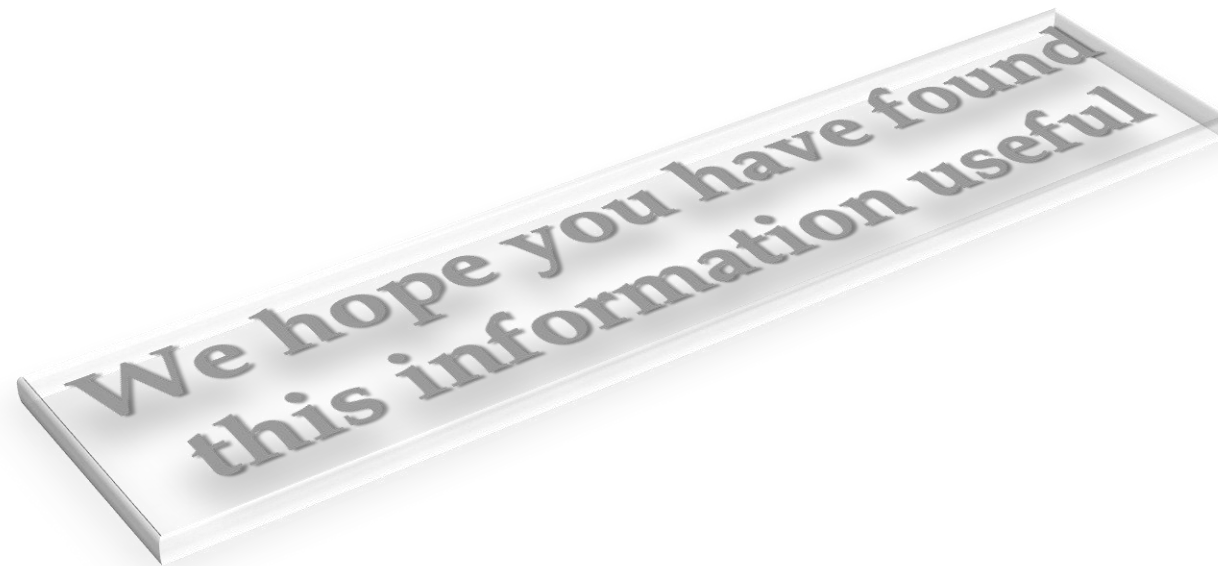
Common Fraud Scams



- ✓ You should not send a wire transfer to receive a loan or a credit card.
- ✓ Fraudulent checks and money orders are used to establish confidence in the validity of the scheme.

Down Payments Execution Guidelines

- ✓ If the request is on behalf of one of your colleagues or managers, verify that the sender has the exact email address that you expect them to have (no additional or missing spaces, underscores, scores, dots or any other marks).
- ✓ Investigate the purpose of the payment and get verification from an internal process owner in your Company. Do not use the "reply" option to reply to the sender, as you may find yourself corresponding with the suspected fake sender:
 - If the down payment is related to a future service, ask for pre-approval from the service recipient to assure they recognize the payment.
 - If the down payment is related to an inventory purchase, receive a signed Purchase Order (PO) and lead time needed from the inventory owner.





Thank You!

Please feel free to contact us for any further assistance,

Chaikin Cohen Rubin & Co. Certified Public Accountants (Isr.)

+972-3-6489858

Moshe Cohen, CPA - Senior Partner

moshe@ccrcpa.co.il

+972-73-2252201

Vered Israelovitz, CPA - Partner

vered_is@ccrcpa.co.il

+972-73-2252241

Ravit Shtrozer, CPA - Partner

ravitsh@ccrcpa.co.il

+972-73-2252211

