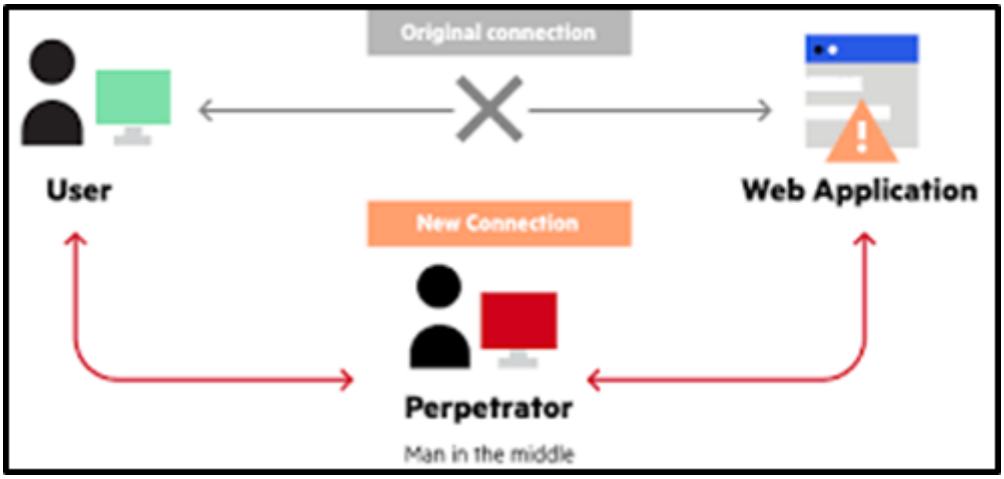
Specialised Security Services

PROJECT:
EMAIL INTERCEPT SCAMS ON THE RISE

Increasingly more businesses are falling victim to the "man in the middle" email intercept attacks that have been on the rise over the past few years.

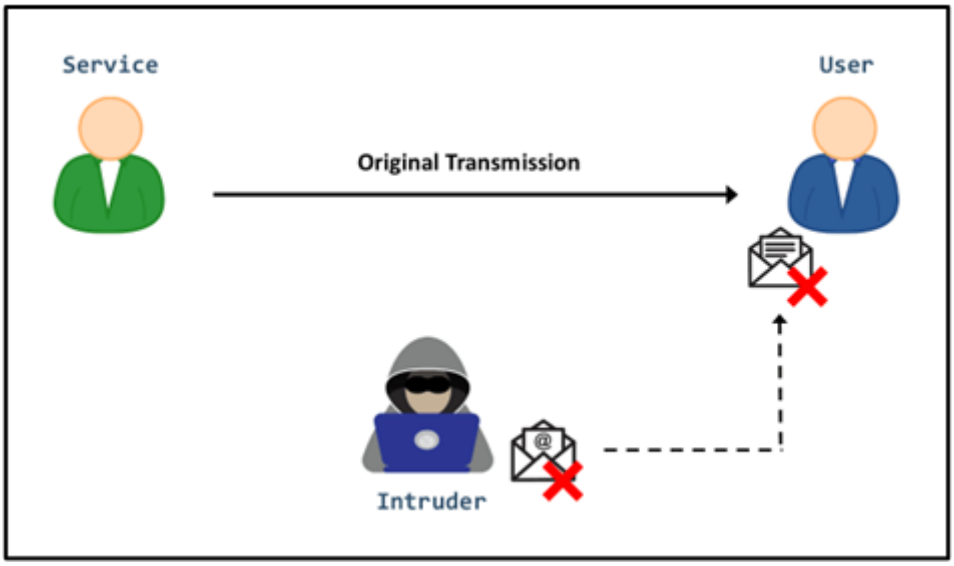
EMAIL INTERCEPTION:

- Email interception is not only a simple matter of someone gaining access to your email login details, and then using your email account to contact someone else, it is far more complex.
- Think of email interception as having a one-on-one conversation with someone employing a third party to do the actual speaking whilst parties 1 and 2 write down what message party 3 should deliver to the other party.
- This sounds like a game we used to play as children, the only difference is that in these instances, party 3 is a criminal with malicious plans of delivering his own version of the message to the other two parties.



HOW IS EMAIL INTERCEPTION SET UP?

- Access to your email domain is gained by means of a phishing scam and/or manipulation tactics.
  The email interception is then set up to allow the party with malicious intent to monitor all incoming and outgoing email communication on the account.
- From that point onward the person will monitor a conversation of interest and insert himself into the conversation at exactly the right time to either gain access to private information or to manipulate the conversation for financial gain.
- The danger is that you as the user will remain unaware of the fact that you are no longer speaking to the party you initiated the conversation with, and that that party is no longer speaking to you.



THE FOLLOWING EXAMPLE IS A CURRENT CASE THAT WE ARE USING FOR ILLUSTRATION PURPOSES:

- Business 1 delivered a service to Business 2 and subsequently sent Business 2 an invoice for services rendered but the email containing the invoice was intercepted by John.
- John proceeded to manipulate the invoice and changed the banking information on the invoice.
- John also proceeded to add a line of text to the original email wherein he requested Business 2 to use the new banking details for all future transactions.
- Business 2 found the email suspicious and replied to Business 1 asking if the banking details were, in fact, correct.
- The return email was intercepted by John who stopped the email from reaching Business 1.
- John then replied to Business 2 posing as Business 1 and sent a fake "proof of bank account ownership" letter to Business 2 along with clear instructions that the banking details were to be changed as requested.
- Business 2 accepted the information and (unwittingly) made the payment to John instead of Business 1.
- A week later business 1 sent an email to Business 2 asking why the payment had not been made yet.
- John intercepted the email and responded to Business 1 - posing as Business 2.
- The email response to Business 1 allowed John enough time to empty the bank account that he had used to commit the fraud.
- Business 2 was also unaware of any complaints from Business 1 about the payment.
- Once John had confirmed that the bank account was emptied and his venture was successful, he ended the intercept, and it was only ***then*** that Business 1 and Business 2 realised that they had been defrauded.

SAFETY MEASURES TO AVOID FALLING VICTIM TO EMAIL INTERCEPTION:

- Never accept a banking detail change without confirming via telephone call and/or in person with the other party that the change is legitimate.
- Never click on unfamiliar links that you receive via email.
- If you receive an email prompting you to change or confirm your login details, exit the email, and visit the applicable website directly to change your details.
- Never accept email as the only form of communication between yourself and another party.
- Always be thorough when sending an email or when replying to an email.
    - Be vigilant of small changes in an email address, for example: ”john123” in the first part of a legitimate email address might be replaced with “j0hn123” in a fraudulent email address.
- Always focus on the small details, like minor changes in an email letterhead, a sudden change of contact information or a sudden change in the use of grammar and/or punctuation.

Specialised Security Services invites the public to the Mike Bolhuis Daily Projects WhatsApp Group.

This group is important in delivering insights into the latest crime trends, awareness, warnings and the exposure of criminals.

HOW TO JOIN THE MIKE BOLHUIS DAILY PROJECTS WHATSAPP GROUP:

- Simply follow the link to our dedicated WhatsApp group:
  - https://chat.whatsapp.com/Dys4JLOFTXCBgXBdXeEvzU
- "JOIN" to ensure you never miss our daily updates.
- You will receive automatic notifications as soon as a new project is placed.

CONTACT MR MIKE BOLHUIS FOR SAFETY AND SECURITY MEASURES, PROTECTION, OR AN INVESTIGATION IF NEEDED.

ALL INFORMATION RECEIVED WILL BE TREATED IN THE STRICTEST CONFIDENTIALITY AND EVERY IDENTITY WILL BE PROTECTED.

You may forward this document.

Regards,

Mike Bolhuis
Specialist Investigators into
Serious Violent, Serious Economic Crimes & Serious Cybercrimes
PSIRA Reg. 1590364/421949
Mobile: +27 82 447 6116

E-mail: mike@mikebolhuis.co.za
Fax: 086 585 4924
Follow us on Facebook to view our projects -
https://www.facebook.com/MikeBolhuisOfficial

EXTREMELY IMPORTANT: All potential clients need to be aware that owing to the nature of our work as specialist investigators there are people who have been caught on the wrong side of the law - who are trying to discredit me - Mike Bolhuis and my organisation Specialised Security Services - to get themselves off the hook.

This retaliation happens on social media and creates doubt about our integrity and ability. Doubt created on social media platforms is both unwarranted and untrue.

We strongly recommend that you make up your minds concerning me and our organisation only after considering all the factual information - to the exclusion of hearsay and assumptions.

Furthermore, you are welcome to address your concerns directly with me should you still be unsatisfied with your conclusions. While the internet provides a lot of valuable information, it is also a platform that distributes a lot of false information. The distribution of false information, fake news, slander and hate speech constitutes a crime that can be prosecuted by law. Your own research discretion and discernment are imperative when choosing what and what not to believe.

STANDARD RULES APPLY: Upon appointment, we require a formal mandate with detailed instructions. Please take note that should you not make use of our services – you may not under any circumstance use my name or the name of my organisation as a means to achieve whatever end.

POPI ACT 4 of 2013 South Africa: Mike Bolhuis' "Specialised Security Services" falls under Section 6 of the act. Read more here: https://mikebolhuis.co.za/popi-act-4-of-2013-section-6-mike-bolhuis/

SSS TASK TEAM:
https://mikebh.link/sss-task-team

SSS CYBERCRIME UNIT:
https://mikebh.link/sss-cyber-team

Specialised
Security Services

Copyright © 2023 Mike Bolhuis Specialised Security Services, All rights reserved.
You are receiving this email to inform and keep you up to date with violent and/or economic crimes. So that you can inform and protect your loved ones and everyone you know.

Our mailing address is:
Mike Bolhuis Specialised Security Services
PO Box 15075 Lynn East
Pretoria, Gauteng 0039
South Africa
Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.

This email was sent to mike@mikebolhuis.co.za
why did I get this? unsubscribe from this list update subscription preferences
Mike Bolhuis Specialised Security Services · Plot 75 Leeuwfontein · Pretoria, Gauteng 0039 · South Africa