****

**SPALSH SCREEN WITH BRAND NAME IMAGE / LOGO AND WEBSITE INFORMATION  
Welcome to Dexpose.com**

**course on email security.**

**In this course, u’ll learn to protect yourself and your customers from BUSINESS 2 BUSINESS scams that occur as a result of inadequacy of electronic mail. (Show two disgruntled business men from mainland china and Europe)**

**You will see;**

***Why email is inherently insecure.* . (Show an email screen briefly)**

***How b2b communication can be compromised***

***and the MODE OF OPERATION of Scam Artists who constantly defraud international business persons in the online B2b marketplace. (Show the interruption by a fraudster)  
  
You will learn about What companies providing email are doing to protect you,*(Show a google protect page)**

***And more importantly, how u can protect urself.***

**Companies providing email are doing a very good job of protecting you {technically}…BUT the focus of this course will be on how u can protect yourself as a business person using email.**

**Ideas in this course are presented on slides…**

**Occasionally u will find links to additional resources for ideas that r technical and beyond the scope of this training. Those links will appear in slightly faint text than TEXT ON the rest of the slide and will be underlined to show that there is a link to an external resource. You can follow the links if you enjoy technical reading.**

**(Show a slide carrying one of the hyperlinks and then move the mouse to indicate the use of the hyperlink. (do this with CPVC) on say PowerPoint or Captivate.)**

**Also; we will adopt a case study approach- showing business characters (buyers and sellers), and email communication between them detailing how to spot an interruption by a fraudster.**

**Show a slide carrying 2 individuals one from asia and the other from Europe and email conversation between them,**

**Slide one =================================================**

Email is the most pervasive method of communication on the Internet –. being “on the Internet” means having an email address; they’re our IDs, how we sign up for things, how we receive notices, and how we communicate with each other. For the most part, using the internet means using email. But there is a very important Question, is email the ideal communication tool for business. Well, to be honest, The Answer is Yes but also No… No because As you will see email is inherently insecure and Yes because you’ll hardly do business online without email.

*From the event* of sending a rfq to receiving a quotation *you will need email*  
from sending purchase order to receiving proforma invoice  
issuing of shipping copies like Draft of B/L or courier copies like AWB.  
Sending and receiving of payment copies.

Email will remain hugely significant

(*Slide one showing moving messages and numbered / bulleted activity log appearing as the messages move, plane carrying documents move and then as goods are being shipped*)

**Slide Two==================================================**

**E**mail is supposed to enhance business communication.

But the reverse becomes the case when communication between a *seller* and a prospective *buyer* is interrupted by a fraudster using the contemporary “Man in the middle attack” somewhat sophisticated *fraudsters* in a manner that can be described as a “*man in the middle attack”.*

*(Show second slide with the bad guy in the middle).*

**Slide Three=================================================**

Internet communications are not always secure. There are lots of attacks on the internet, and with Email being a significant target, B2b email users are better off armed with information that will help them protect their business communication from prying eyes.

*(Show a conversation between disgruntled business men from Asia and Europe.)*

This course/presentation seeks to uncover the mode of operation of Business to Business (B2B) email scams that currently plague international businesspersons in established online B2B platforms. So follow along carefully as we demonstrate in the video series how ur b2b communication can be interrupted. For those who have lost some money as a result of such interruption…this course will be an eye opener and might save you another loss. And for those with no experience of interruption you can save your company from an imminent loss by following as we demonstrate. Welcome once again.

**Slide Four =================================================**

**WHY WE NEED EMAIL?**

Email addresses are extremely valuable in today’s economy. Our Identities, important account and vital information are tied to our email addresses. Chances are your financial institutions use your email address as your username. Your social media accounts like twitter and facebook tie to your email address. Your email address is a unique identifier. But more importantly it is a communication mechanism. ([*http://www.slideshare.net/mailchimp/email-security-14045169?from\_search=1*](http://www.slideshare.net/mailchimp/email-security-14045169?from_search=1))

Email will remain hugely significant, surpassing Telephony and Postal Service as a communication tool in the B2B ecosystem. Since using the internet also means using email, email gives us access to more business prospects. Messages are also delivered faster than the traditional post. Ability to deliver messages together with necessary business documents (*as attachments*) in several file formats is also a great feature. Also, phone calls between people of different languages and cultures (*as is usually the case between buyers and sellers in B2B scenarios*) do not give enough room for expression of interest and offering as a result. With email there is enough time for a seller to scrutinize a buyer’s request for quote and as such present a suitable offering. Email will remain the Ideal business communication tool -- **🡪**

But the issue of security needs to be tackled else doing business online will be painful for a lot of people… at dexpose we believe email security starts with you, the user.

**Slide FIVE ==================================================**

**AN INHERENT PROBLEM (Your Email can be compromised)**

**Email can be accessed in one of two ways either using a Client Application on desktop computer (like Microsoft Outlook, Thunderbird) or using a webmail service like Gmail, Yahoo, and Microsoft Hotmail.**Today, there are four basic places where most people’s email can be compromised:

**(For first caption).**

* On your device(s)
* On your recipient’s device(s)
* On the networks
* On the server(s)

The first and last places – devices – are easy to understand. If someone can sit at your computer, grab your phone, or swipe through your tablet, odds are that your email is sitting right there for them to read – You do use a lock screen or password on your devices, right? Same thing goes for your recipients’ devices. But even passwords and lock screens sometimes aren’t much help. While a few email programs encrypt the email messages they store on the device, most don’t. That means anyone (or any program) that can access the device’s internal storage can probably also read email and get to file attachments.

It doesn’t have to be a person;

Because Rifling through email is one of the most common things malware does**.**

**(For second caption).**

Type of connection http or https used by your email service provider

If the connection to your WebMail server is “insecure” (i.e. the address is http:// and NOT https://), then all information including your username and password is not encrypted as it passes between the WebMail server and your computer gladly http:// for webmail is a thing of the past…not so many webmail providers use that anymore…if u notice ur company uses a webmail CONNECTION that’s NOT SECURE PLS DO WELL TO SWITCH TO A MORE SECURE CONNECTION,

**(For third caption).**

Limitations of SIMPLE MAIL TRANSFER PROTOCOL (SMTP).

The mechanism and language (i.e. protocol) by which one email server transmits email message(s) to another email server is called SMTP (Simple Mail Transport Protocol).

The inherent strength of Electronic mail is also matched with as much weakness.  
verification is a problem as u will later see. There is no way to immediately verify that a message truly came from a certain address. Authentication –

**(For fourth caption).**

Email is overly insecure as we will see in this report. There is no unobtrusive (apparent) way for a person who receives a message to ascertain that the message came from where it claims to have come from.

For a long time now, email servers have had the option of using Transport Layer Security, TLS and other email security tehnologies like  [PGP and S/MIME](http://luxsci.com/blog/the-case-for-email-security.html)) to *transparently* encrypt the message *transmission* from one server to the other. Use of TLS with SMTP, when available, ensures that the message contents are secured during transmission between the servers. Sadly,

Not all servers support TLS!  Use of TLS requires

The purchase of one or more SSL certificates  
configuring the email servers to use them  
additional computational resources on the email servers involved.

For these reasons, many email servers, especially free or public ones,*do not support TLS* at all (though there is a steady trend toward TLS support; e.g. gmail used to not support TLS, but now they do).

**(For fifth caption).**

Email can also be compromised as a result of As a result of laxity and naivity in the part of the user. The use of outdated antivirus software can allow malware to compromise the user’s system but also ignorant release of personal information and response to phishing pages is also a major cause of compromise.

**===================================================================**

**Slide six  
 ==================================================**

**Email scams resulting in huge financial loses usually start when any of buyer or seller identities is compromised by a conman. And communication interrupted.**

**What happens when communication btw a buyer and a seller is interrupted by a fraudster**

1. **Buyers lose their monies**
2. **Sellers lose reputation as there’s is no apparent way to say I didn’t scam you.**
3. **Sales men lose their jobs as they cannot prove the message was not sent from their mailboxes sometimes a sales person can be sent to court or prison.**
4. **Online B2b marketplaces become less attractive for affected business persons particularly buyers.**
5. **And since the internet and email is definitely needed in today business climate… the affected parties lose business volume as a result of insecurity.**

**Slide seven ==================================================**

Whilst there is a lot of work being carried out by information service providers like google, yahoo, and other email service providres to protect our information, especially in the srea of encryptioni a lot of responsibility still lies on the uers like ourselves to help protect our own information from attacks that even the technology giants cannot protect you from.

**A FIRST AID SOLUTION TO INSECURECURITES PRESENTED BY EMAIL**

1. Never rely on email alone.  
   Follow important messages with a phone call or SMS…Skype too is very important
2. For buyers: Never take a change of account information from seller likely the message might not be from your supposed seller u might be on ur way to becoming a victim
3. Copy as many partners as possible and suspect an impending interruption if concerned partners are not copied in a sensitive information exchange.

For an international businessman who leverages the Online B2b marketplace and Electronic mail, A proper and useful combination of the three business communication tools highlighted above is what he/she will need to ensure that communication between his buyers and/or sellers are effective but also secure. One will not be able to rely on email alone except you adopt certain preventive strategies as will be shown in the accompanying presentation.

Salesmen and other business communication personnel who do not acknowledge the presence of email scams in online B2B marketplaces will remain a sitting target for costly security attacks resulting in huge financial losses. **🡪**

**This presentation will not bore u with all the technical details about why email is insecure for technical details kindly visit the following online resources and if u have subscribed to this course don’t forget to read the accompanying documents sent to your email .**

**EMAIL SCAMS IN B2B MARKETPLACES- THE EXPOSE**

**Present all the ideas here below in slide format, forward and backward swiping between slides and demonstration as the ideas presentation progresses but also showing progression of presented ideas.**

**O**nline B2B marketplaces usually require Sellers (*Suppliers, Companies,and Manufacturers)* and Buyers to register and create their profiles online. As part of the registration, the Buyer or Seller is required to provide an email address that will serve as messaging tool in the course of their transaction with other buyers and sellers. Registrations are usually free so there is little or no investment required by intending fraudster.

The Scam Modus Operandi goes thus;

1. Email address Sourcing: Like every normal buyer a Buyer with an intention to defraud will source for products from suppliers using the search provided by an online B2B marketplace*. While it might appear as though it a product sourcing activity, it is actually email address sourcing*. After search results show up, the scammer checks the companies that appear with every search result and asks for a RFQ. The aim here is to contact as many suppliers as possible in a process nicknamed bombing! Of course, suppliers who receive the RFQ will have to reply by email. more replies from suppliers translate to access to more email addresses Thus increasing the chances for successful attacks.

To protect identities of buyers and sellers B2b sites usually limit the no of RFQs that can be sent by…some b2b sites like europages have Since November Europages.co.uk has discontinued the idea of checking multiple suppliers to contact most likely in the bid to reduce the bombing. Of course scammers do not resort to bombing sites for gathering of email addresses they can also buy email leads from others online who r in the business of selling email addresses…why r ur email addresses so important….lets find out.

**BOMBING** ---show images from alibaba.com…europages.com…globalsources.com…

1. Messages of RFQs together with contact information of the buyer are automatically sent to all the sellers’ email addresses - obviously the email addresses they provided in the course of registration as members of the B2B marketplace. The idea is that the sellers will thereon have to contact the buyers directly. One thing to note here is that RFQs from Scam Buyers are never detailed and the seller is moved to write the buyer to ask for more details like a picture or any document describing the product in the request. This is where it all heats up.
2. **Phishing**: In this stage the scam buyer tries to steal the password of sellers using the effective phishing techniques or other more sophisticated Trojan-Horse botnet attack.  
   below is an email message from a scam buyer to a seller in reply to the seller’s request for more details discussed in 2. above

…

2nd format…in a mail program showing link and attachment

…

In a phishing attack the seller is required to click a link or download an attachment in the message to view the detailed specifications of the buyer’s request. The link directs the seller instead to enter his password into a login screen that has a striking resemblance to the original login screen that they use in gaining access to their inbox

*(Visit* [*http://www.kennethetal.com/b2b-scam-expose/phishing-pages*](http://www.kennethetal.com/b2b-scam-expose/phishing-pages) *to give yourself a feel of the phishing attack)* … discuss spyware if necessary or state that its outside the scope of this work.

For an unsuspecting seller the result is loss of password to fraudsters as they are redirected to some page on the worldwide web where they left to wonder what to do next until they give up on the buyer and move on.

1. Armed with the passwords to email address of sellers (*usually the sales department email*)the scammer gains entry into the inbox of the seller and this is where it all heats up. After studying messages in the Inbox and Sent Folders of the seller,the scammer makes a list of all buyers who have indicated a genuine interest to buy and pay for goods being produced for them. A mind blowing trick nicknamed **CLONING** follows.
2. **Cloning** involves exploitation of common sense. To clone an email address the scammer creates an email that has a striking resemblance to the sellers’ email for example

Looking at an email address [wangcho@gmail.com](mailto:wangcho@gmail.com) a clone [vvangcho@gmail.com](mailto:vvangcho@gmail.com) will be created.

Looking closely, you will see that the first email address begins with a “w” whereas the second email begins with a “v” followed by another v that makes it look like a “w”

In the course of demonstrating the expose we will adopt a documentary *APPROACH SHOWING CHARACTERS OF BUYERS AND SELLERS (NOT THEIR REAL NAMES)* AND COMMUNINCATION BETWEEN THEM.

EACH EPISODE FOLLOWS WITH A LESSON OF DOs AND DONTs SO FOLLOW along closely and enjoy the expose.