

ShipServ Information Security Awareness



| | |
|---|----------|
| Introduction..... | 1 |
| 1 CUSTOMER DATA SECURITY | 1 |
| 1.1 WHAT DATA IS CONSIDERED SENSITIVE OR CONFIDENTIAL? | 1 |
| 1.2 LABELLING, HANDLING AND DISTRIBUTION OF SENSITIVE DATA..... | 2 |
| 1.3 DISPOSAL OF SENSITIVE DATA..... | 2 |
| 1.4 APPROVAL POLICY FOR CUSTOM DATABASE REPORTS..... | 2 |
| 1.5 ACCESS TO PAGES SUPPLIER INSIGHT REPORTS (SIR) | 2 |
| 2 INTERNET AND COMPUTER SECURITY | 3 |
| 2.1 WEB BROWSING SECURITY | 3 |
| 2.2 E-MAIL SECURITY | 4 |
| 2.3 INSTANT MESSAGING SECURITY: SKYPE AND WINDOWS MESSENGER | 4 |
| 2.4 SCAMS AND HOAXES | 4 |
| 2.5 PASSWORDS AND ACCOUNTS SECURITY | 5 |
| 2.6 PC AND LAPTOP SECURITY | 5 |
| 2.7 LAPTOP PHYSICAL SECURITY..... | 6 |
| 2.8 WI-FI SECURITY | 6 |
| APPENDIX A. CONTACT DETAILS | 7 |
| Appendix B. examples of fraudulent e-mails, fake warnings etc. | 7 |
| a. example of fraudulent Skype message..... | 7 |
| b. example of forged e-mail containing malicious link : | 8 |
| c. Example of fake security warning : | 8 |
| d. Examples of fake browser-popup warnings | 8 |

Introduction

This document outlines security requirements and responsibilities for ShipServ staff, and gives practical advice for applying good information security practices during the course of their daily work. This includes requirements on handling sensitive customer data, as well as more general IT-related security advice.

It's important to stress that information security awareness affects all staff on a daily basis, and that means **YOU!**

If you are in any doubt about the issues raised by this document, please feel free to ask the ShipServ Information Security Officer or IT Support - see Appendix A for contact details.

1 Customer data security

ShipServ stores a significant amount of information about its customers, including sensitive business-related financial information related to each customer's trading activity: trading volumes, trading relationships between customers, product pricing and discounts etc.

It is of paramount importance that ShipServ staff must treat this customer data as confidential, and do not allow it to fall into the wrong hands. Failure to comply with the following requirements may be cause for dismissal.

1.1 What data is considered sensitive or confidential?

Any customer information which is not already made public by the customer should be considered as confidential: here are some examples:

- details of customer trading activity : lists of transaction volumes, GMV or trading partners of a customer;
- prices contained inside customer Quotes, Purchase Orders or other documents;
- customer usernames and passwords;

- **any report obtained from ScoreCard, WebReporter, Supplier Insight Reports or SalesForce;**
- any customer-specific data extracted from the ShipServ TradeNet database.

In addition, any financial data about ShipServ the company should also be considered as sensitive:

- ShipServ annual revenue/turnover , profit/loss details, share price, company financing details;
- revenue per ship, cost of sales per ship, or what fees customers are paying ;
- details of our share option programmes.

1.2 Labelling, handling and distribution of sensitive data

The following practices must be followed:

Distribution of any data listed under section 1.1 above is not permitted, with the sole exception of sharing data on a specific customer with an authorised employee of that same customer

If you are producing a report or document containing confidential information, please label it “ShipServ Confidential” before distributing it.

Don't leave print-outs with sensitive information lying on your desk or in other visible areas such as meeting rooms or near printers.

Clear your desk before you leave work in the evening, and put away any documents containing sensitive information in a locked drawer or cupboard.

If you are printing a document containing sensitive information, make sure you know which printer it will be printed on, and go and collect the print-out immediately from the printer.

1.3 Disposal of sensitive data

If you have printed out sensitive or confidential information and no longer need to keep the printed copy, please dispose of it using a paper-shredder. Do not put it in the wastebasket or paper recycling bin.

1.4 Approval policy for custom database reports

Occasionally as part of your duties you may require additional customised information to be extracted from the ShipServ TradeNet databases by the IT team – for example, data which is not available in the standard ScoreCard reports nor in Supplier Insight Reports.

Only staff who have been specifically authorised to request these ‘custom database reports’ may do so. The ShipServ Chief Operating Officer authorises who is on this list of ‘authorised users’ – currently restricted to senior members of the Global Service Delivery team.

1.5 Access to Pages Supplier Insight Reports (SIR)

Access for ShipMates to run SIR reports is only permitted from ShipServ offices, since ShipMates’ accounts are able to run SIR reports on any customer.

However if you are working from home or in a hotel on a business trip, you may request that your location is temporarily added to the list of locations with permission to access SIR – please contact David Hardy or Robin Sinclair for approval, with details of your current location , and IT Support can set this up for you.

N.B. if you are at a customer’s office and wish to run SIR for a customer, please do not request that the customer’s office be added to the list of approved locations , since this represents a security risk if your account is compromised – instead, get the customer to log in to Pages and show him/her how to use SIR.

2 Internet and computer security

Most of ShipServ's daily business takes place via the public Internet, where there are various risks to the unwary user: viruses and other malware, as well as numerous scams and hoaxes.

This section provides guidance for staff on how to use the Internet safely and reduce the risk of becoming a victim of these security threats.

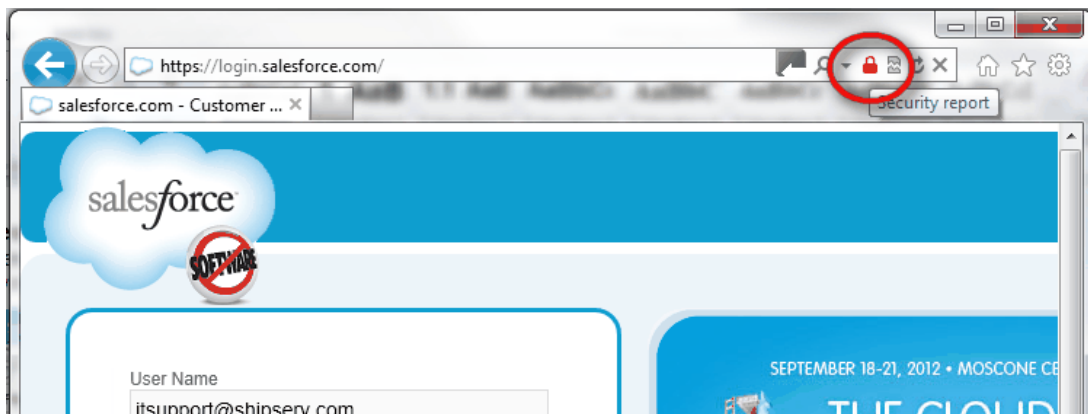
Most of these tips are also valid for general use of the Internet at home or elsewhere.

2.1 Web browsing security

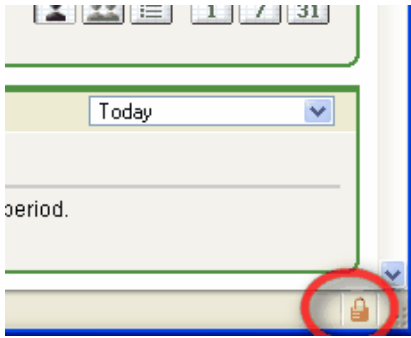
- Before browsing the Internet, make sure that your web browser (Internet Explorer) is up-to-date with security updates – see section 2.6 below for details on how to check Automatic Updates is On.
- Upgrade to the latest version of Internet Explorer if you can, as it should be the most secure. Currently the latest is version 8.
- Use caution when visiting websites which you have not used before – remember that clicking on a link may permit the website to install spyware or other unwanted programs on your computer. In particular, please be aware of the following tricks :
- **Watch out for adverts masquerading as Security Warnings** – if you see a flashing message telling you that your computer is infected, this is unlikely to be genuine.
- **Become familiar with what your anti-virus software does when it encounters a virus** or malware. You can visit the following link to download a harmless test-virus file which should activate your anti-virus program's pop-up warning :

<http://www.eicar.org/download/eicar.com>

- **Avoid offers too good to be true.** if you find a low-priced item or 'special offer' on a website that you're not familiar with, proceed with caution : just because a website shows up near the top of the Google search results doesn't mean it's safe to buy from it.
- **install a website-checker tool** into your web-browser : this will help you identify and avoid suspicious websites. One such tool is **McAfee SiteAdvisor** which works well with Internet Explorer – visit www.siteadvisor.com for more details and instructions on how to install it. This tool marks safe websites with a green tickmark in the Google search results, and allows you to check any website to see if it has any known security problems.
- **Take care when entering credit card details** or other private data on a website – make sure that the website address starts with **https://** (rather than **http://**) and that there is a little gold-coloured security padlock showing in the browser :



The screenshot above shows the golden padlock in Internet Explorer version 9 : in other browsers or older versions of Internet Explorer, the gold padlock may be shown at the lower-right of the browser window:



2.2 E-mail security

The key points to note include:

- Don't open attachments on e-mails from people you don't know.
- Use caution when opening unusual attachments to e-mails, even if the e-mail appears to come from a colleague. The sender may be forged and the e-mail was not really sent by your colleague.
- If in doubt, it is best to maintain a suspicious attitude: remember that an e-mail may not be from who it appears to be from – e-mail is not 100% secure and it is not difficult for someone to forge the 'sender' address on an e-mail.
- To virus-scan an attachment before opening it, first save the attachment file to a temporary folder on your PC and then run a virus scan on it.
- If you receive an e-mail sent to you by mistake which was intended for another person, you should delete the e-mail and inform the sender of his/her error. You may not forward the e-mail to anyone else.
- Never reply to spam e-mails. Never click on links in spam e-mails, even if it appears to be a link to unsubscribe. Where possible, avoid opening spam e-mails altogether.

2.3 Instant messaging security: Skype and Windows Messenger

Instant Messaging programs such as Skype and Windows Messenger can be abused to send malware by unscrupulous users, so please treat with suspicion any unexpected chat messages you receive – for example, a message informing you that your computer is infected and asking you to “click on the following link” or similar. Even if the message comes from one of your known contacts – they may have fallen victim to a malware themselves.

See Appendix B below for an example of a fraudulent Skype message.

2.4 Scams and hoaxes

The best way to avoid Internet scams is to read about the more common types of scam and be aware of the forms they take. Here are some links to more information on this topic: please spend half an hour or so to read through these and become familiar with the techniques used by scammers:

<http://www.onguardonline.gov/topics/email-scams.aspx>

http://www.wiredsafety.org/scams_fraud/

<http://www.hoax-slayer.com>

If you receive an e-mail from a friend which contains an alarming warning of some kind, and asks you to urgently forward it to everyone you know, this is most likely a hoax.

2.5 Passwords and accounts security

During the course of performing their duties, ShipServ staff may use accounts on multiple different computer systems, both ShipServ-operated systems and third-party systems such as Salesforce.com or our outsourced Microsoft Exchange e-mail server.

Employees are responsible for maintaining the privacy and security of these accounts, and should not provide their passwords or other security details to other people.



Passwords should be secure, and changed regularly. A secure password uses a mix of lowercase and uppercase letters, plus numbers and punctuation - for example: **Chav.66** or **giMe\$50**

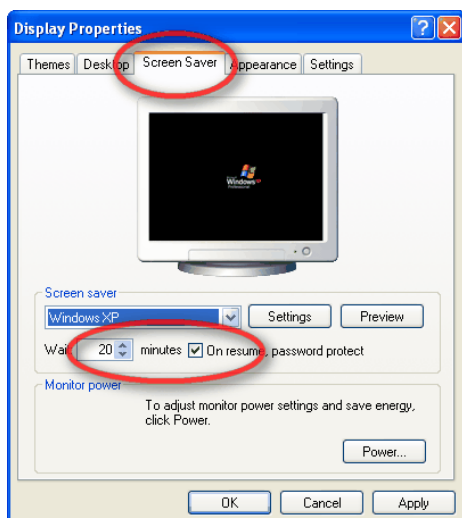
If you have reason to believe an account has been compromised or that your password has become known to someone else, please inform ShipServ IT support and the ShipServ Security Officer.

2.6 PC and laptop security

As the principal user of your ShipServ computer, you are responsible for certain aspects of its security.

Here are the key points to follow :

-  Ensure that you have a secure and difficult-to-guess login password on your computer.
-  Ensure that you have an up-to-date antivirus software installed and running. *In Microsoft Windows, Start -> Control Panel -> Security*
-  Always virus-scan any program or file you download from the Internet, even when it appears to come from a well-known or trusted source.
-  If you suspect your PC may have been infected by some kind of malware, please inform IT support.
-  Make sure that a firewall is installed and running on your computer. *In Microsoft Windows: Start -> Control Panel -> System and Security (or in Windows XP: Start-> Control Panel -> Windows Firewall)*
-  Ensure that your PC is set up for Automatic Updates. This will download fixes for any security holes which Microsoft detects in Windows and Internet Explorer. *In Microsoft Windows: Start -> Control Panel -> System and Security (or in Windows XP: Start-> Control Panel -> Automatic Updates)* . You can also run Start -> Programs -> Windows Update to manually check for updates.
-  If you use Microsoft Office, use “Microsoft Update” instead of “Windows Update”, to receive security fixes and updates for Microsoft Office as well as for Microsoft Windows. *In Microsoft Windows: Start -> Programs -> WindowsUpdate , and choose to receive “updates for other Microsoft products” (in Windows XP, follow the instructions to install ‘Microsoft Update’)*
-  If you have to leave the room while using our computer , use the screen-lock feature to prevent others accessing your computer in your absence. *In Microsoft Windows, simply hold down the ‘Windows button’ (at lower left of the keyboard) and press the “L” key.*
-  Set the “password protect” option on your screensaver. *In Microsoft Windows, right-click on your Desktop and choose ‘Personalize’ or ‘Properties’, then go to the ScreenSaver tab :*



Certain other popular commercial programs are also targeted by viruses and malware, so please ensure that you keep other programs up-to-date with security patches: Adobe Reader, Adobe Flash Player, Java etc. ShipServ IT support can help you with this, and will also send out warnings to all staff if urgent or important security updates need to be applied.

The above tips can also be used for your personal computers at home.

2.7 Laptop physical security

A few additional tips for laptop users:

- Be careful when travelling – never leave your laptop unattended. Keep a close eye on it during airport security checks.
- Use a laptop security cable (also known as a “Kensington lock”) to attach your laptop to your desk.
- Never leave your laptop visible inside a vehicle.
- Never leave your laptop in a vehicle overnight, even if it is not visible.
- Make sure any important data on your laptop is backed up regularly, ideally onto a server in the office.

2.8 Wi-Fi security

When out of the office or travelling, you may have to use public wireless networks to access the Internet. Here are a few tips to stay safe:

- Make sure your Windows firewall is on before using any Wireless network;
- Avoid fraudulent wi-fi networks: if connecting to a wireless network in a hotel, airport or Internet café, ask a member of staff to confirm the name (or “SSID”) of the wireless network, before you connect to it.
- Only connect to wireless networks which are marked as “security-enabled” (a little padlock symbol should be shown against secure networks). This symbol means that your wireless communications will be encrypted and malicious wireless users will be unable to view your traffic.
- Take care when entering credit card details or other private data on a website – make sure that the website address starts with **https://** rather than **http://** and that there is a little yellow security padlock showing in the browser as shown in section 2.1 above.

Appendix A. Contact Details

ShipServ Information Security officer: Robin Sinclair rsinclair@shipserv.com +44 20 3051 0263

ShipServ IT Support : itsupport@shipserv.com +44 20 3051 0273

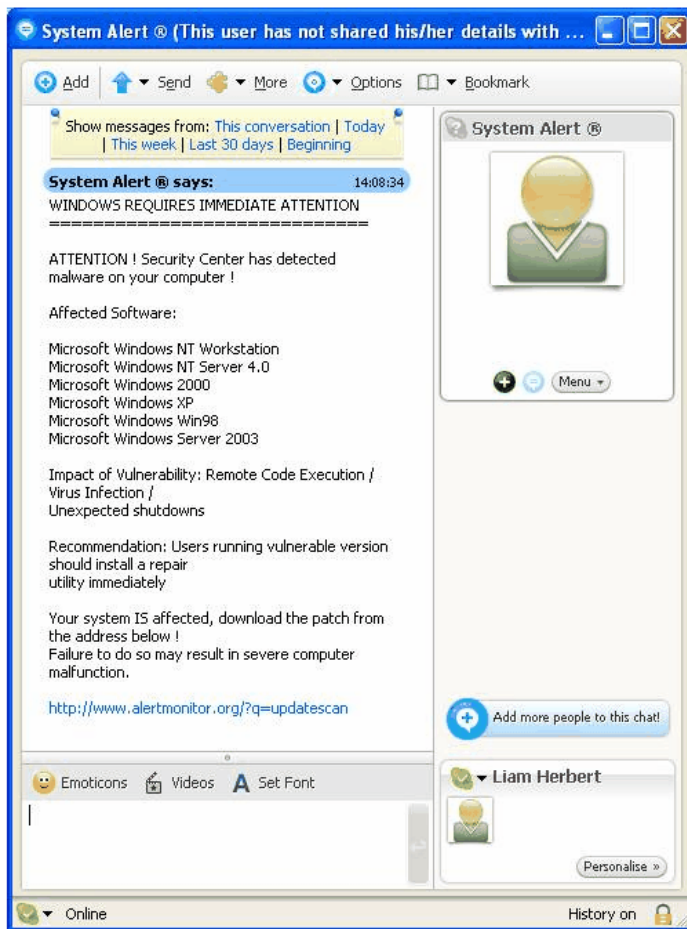
Chief Operating Officer: Kim Skaarup , kskaarup@shipserv.com

Appendix B. examples of fraudulent e-mails, fake warnings etc.

a. example of fraudulent Skype message

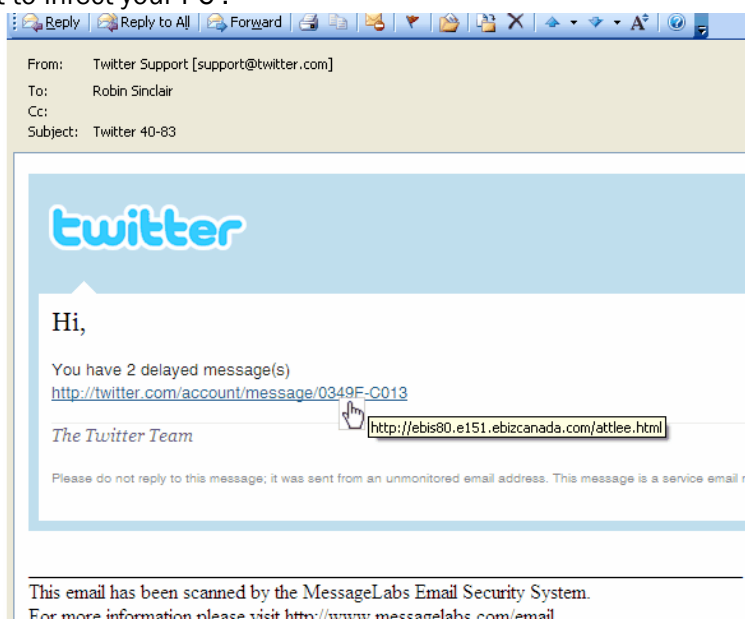
I received the following Skype message which appears to be from one of my colleagues who is one of my Skype contacts. But in fact it was sent without his knowledge by a malicious program on his PC.

If I were to click on the link to www.alertmonitor.org shown at the end of the Skype message below, then I would run the risk of my PC being infected with a virus or other malware:



b. example of forged e-mail containing malicious link :

This appears to be an e-mail from Twitter, but if you hover your mouse over the link in the mail, you can see that the link will not take you to twitter.com but to ebizcanada.com which is probably a malicious website which will attempt to infect your PC :



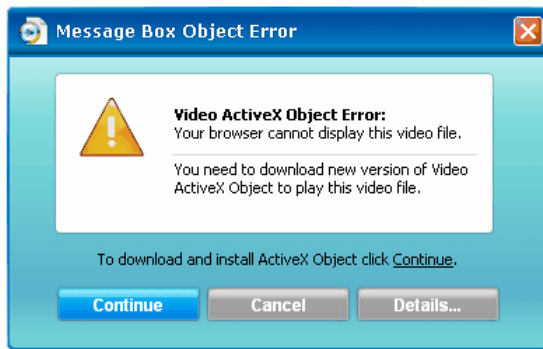
c. Example of fake security warning :

This pop-up window appeared after clicking a link in a Google search results page. It tries to mimic the appearance of the Windows Security Center, but if you click anywhere on the window shown below, it will try to install unwanted software on your PC:



d. Examples of fake browser-popup warnings

These warnings appeared when visiting an online TV website which asks you to download a new video 'codec' in order to be able to view the video clips or TV feeds on the site. The download is likely to do something malicious on your computer.



or

