Queensway Navigation Co. Ltd

Quarterly Safety Bulletin

Cyber Security

This safety bulletin is for:

- Office representatives, Masters and Crew
- Superintendents

Purpose

This safety alert series is a selection of Company's reported near misses, accidents or incidents and aim to share lessons learnt throughout the fleet. Special care has been made in order to safeguard privacy in reported cases. It is recommended to be posted in conspicuous areas on board.

Case History

One of Company's employees clicked on an attachment of an incoming e-mail by a **known** source.

The computer virus was blocked by company's firewall and antivirus system maintained by company's IT dpt.

Route Cause	Less than adequate user supervision / awareness.
Corrective Action	The virus was isolated and deleted by company's firewall and antivirus system maintained by company's IT dpt.
Preventive action	Guidelines on safe e-mail / browsing practices.

Safe e-mail practices

1 Do not open **unknown e-mail attachments**. If a message has attachments, don't open it unless you know the sender and are expecting the attachment. Let me be direct, your antivirus software will not fully protect you. The misconception that running the best antivirus / antimalware software will safeguard you is patently wrong. This also applies when browsing to unsafe websites.

2 Spammers use a wide variety of clever titles to get you to open e-mails which they fill with all sorts of bad things. The majority of e-mail users often make the **mistake of opening these e-mails**. So in an effort to bring you up to speed, let me tell you quickly:

- ✖ You have not won the Irish Lotto, the Yahoo Lottery, or any other big cash prize.
- ✖ There is no actual Nigerian King, Prince or Federal Ministry of Finance trying to send you $10 million.
- ✖ Your Bank Account Details do not need to be reconfirmed immediately.
- ✖ You do not have an unclaimed inheritance.
- ✖ You never actually sent that "Returned Mail".
- ✖ The News Headline e-mail is not just someone informing you about the daily news.
- ✖ There are not any funds ready to release for future investments and projects.
- ✖ You have not won an iPhone 6S.

Safe browsing practices

1 Banks and online stores provide, almost without exception, a secured section on their website where you can input your personal and financial information. They do this precisely because e-mail, no matter how well protected, is more easily hacked than well secured sites. Consequently, you should avoid writing to your bank via e-mail and consider any online store that requests that you send them private information via e-mail suspect.

2 A common technique used by spammers is to send out thousands of fake newsletters from organizations with an "**unsubscribe**" link on the bottom of the newsletter. E-mail users who then enter their e-mail into the supposed "unsubscribe" list are then sent loads of spam. So if you don't specifically remember subscribing to the newsletter, you are better off just blacklisting the email address, rather than following the link and possibly picking up a Trojan horse or unknowingly signing yourself up for yet more spam.

3 While never opening a **phishing** e-mail is the best way to secure your computer, even the most experienced email user will occasionally accidentally open up a phishing email. At this point, the key to limiting your damage is recognizing the phishing e-mail for what it is.

Phishing is a type of online fraud wherein the sender of the e-mail tries to trick you into giving out personal passwords or banking information. The sender will typically steal the logo from a well-known bank, PayPal etc. and try to format the e-mail to look like it comes from the bank. Usually the phishing e-mail asks for you to click on a link in order to confirm your banking information or password, but it may just ask you to reply to the e-mail with your personal information.

Whatever form the phishing attempt takes, the goal is to fool you into entering your information into something which appears to be safe and secure, but in fact is just a dummy site set up by the scammer. If you provide the phisher with personal information, he will use that information to try to steal your identity and your money.

Signs of *Phishing* include:

→ A logo that looks distorted or stretched.

→ E-mail that refers to you as “Dear Customer” or “Dear User” rather than including your actual name.

→ E-mail that warns you that an account of yours will be shut down unless you reconfirm your billing information immediately.

→ E-mail threatening legal action.

→ E-mail which comes from an account similar but different from the one the company usually uses.

→ E-mail that claims “Security Compromises” or “Security Threats” and requires immediate action.

BE PROACTIVE!

✓ Use your **common sense**. Does a website look strange to you? If it looks unsafe, don’t take the risk.

✓ Do not click on **unknown links**. Links may not be what they seem and may redirect you to harmful pages and malware.

✓ Disable **stored passwords**. Nearly all browsers and many websites in general offer to remember your passwords for future use. Enabling this feature stores your passwords in one location on your computer / device, making them easier for an attacker to discover if your system gets compromised. If you have this feature enabled, disable it and clear your stored passwords.

✓ Be cautious on **social networking** sites. Even links that look they come from friends or seem safe, can sometimes contain harmful software or be part of a phishing attack.

✓ Avoid **public or free Wi-Fi**. Attackers often use wireless sniffers to steal users’ information as it is sent over unprotected networks. The best way to protect yourself from this is to avoid using these networks altogether.