DS41 – Internet and Email Security for Clubs

February 2016 –Version 1

We have recently been made aware that an affiliated Club has been targeted by what appears to be fraudsters who have managed to hack in to some of the Club officials email accounts. Acting as the Chairman, they got in contact with the Treasurer and asked for funds to be transferred into a different bank account from the Club account. As most Clubs have websites with contact emails publically available, we would like to warn all Clubs to remain vigilant and be wary of any correspondence you may receive relating to the transferring of funds.

Prevalence Of Whaling / Phishing Attacks Over The Recent Months

Cyber attackers have gained sophistication, capability and bravado over the recent years, resulting in some complex and well executed attacks. But, some of the most successful threat activity remains relatively basic, and uses simple social-engineering to dupe targets. Whaling is a targeted attack that uses the following tactics to exploit its victim:

- Research: Attackers research their target organisations, to identify their victim and the organisational hierarchy around them.
- Spoofed emails: Whaling attacks use email sent from spoofed or similar sounding domain names to yours.
- Social engineering: Whaling emails appear to be sent from the CEO or CFO and are used to trick finance users into making illegitimate wire transfers to the cyber-criminals.

Basic Internet Security Validation Technique for Clubs

- Set up a system of validation questions and answers for use between committee members.
- As a matter of routine, whenever a financial request or release of information is received as an email request, the addressee can expect to receive a previously agreed PIN number or KEY word to be TEXT to the recipient of the email via an agreed mobile phone number.
- For example: A Chairman emails a request to the treasurer for transfer of £250 and then sends a confirmation TEXT with the pre-agreed PIN or KEY WORD
- The Treasurer, if still cautious contacts Chairman by phone to satisfy that the request is genuine

2016 © The British Horse Society. All rights reserved. Please note that all of these datasheets are not to be posted on any public forum. They are an Affiliation benefit.

- Key words should be random and not connected to club name, location or name of committee member. Don't use the year or any membership numbers as PIN numbers
- Another method is to conduct financial business face to face. However this is not always possible on a day-to-day basis.
- If in doubt use another method to contact the person making the request in addition to email.

DO NOT

- Disclose PIN or KEY words in emails
- Disclose Mobile Phone Numbers in emails
- Share this information amongst all members, instead restrict to “Need to Know” committee members only
- Get upset if group member challenges your email and asks for validation
- Ever reply to an email quoting the PIN or KEY words

DO

- Agree a Club policy for use and stick to it
- Change PIN or KEY words regularly
- Change the PIN or KEY words if a committee member leaves

2016 © The British Horse Society. All rights reserved. Please note that all of these datasheets are not to be posted on any public forum. They are an Affiliation benefit.