IMPORTANT NOTIFICATION

Clubs Are Being Targeted By Scammers

It has come to our attention that some clubs and their members have recently been the target of email scammers. These scammers are targeting clubs to gather information then creating a Spoofing and Phishing scheme to trick club members into paying statement balances to incorrect bank accounts. To define these:

Spoofing: When a scammer creates a fake email address to impersonate someone (e.g a staff member).

Phishing: When a scammer attempts to receive personal information (bank account, passwords, or the sending of money) from someone (e.g. a member).

In two reported cases that we have been made aware of, a club employee received a request for information from an email which either appeared to be from another club employee, or was in fact sent from another club employee's personal email account which had been hacked. The request for information included Member Names, Contact Details and Outstanding Balances. In both cases, a similarly worded message was sent to club members.

Excerpt from one of the emails:

This is to inform you that we are currently having problems with the club account and due to the Covid-19 crisis, we may not be able to resolve it before

the weekend. In the meantime, we have designated certain personal accounts to collect payments. You have a total outstanding balance of $7,203.0. We know these are tough times for everyone and this is probably the last thing on your mind, but we are trying to pool funds together to secure enough test kits and make basic supplies reasonably available.

What your club can do:

- Notify your membership to be on the lookout. Remind them of the only way that the club would request or accept payments.
- Create an internal confirmation process between staff that sends sensitive information.
- Enhance email passwords following best practices for password complexity.
- Question and call your fellow employees when things seem odd.
- Verify the addresses of who is requesting sensitive club information and those to who you are sending this information.

At Jonas Club Software, we take security very seriously by investing heavily in proper infrastructure and resources while constantly monitoring our systems. However, your club also plays a huge role in the overall defense of your data and resources. Below please find a couple of tips and tools to help your organization be vigilant about cyber security.

- SSL Certificates
    - SSL certificates provide an added layer of protection to your site, encrypting all traffic sent between the website and your members. This is particularly important to shield sensitive information, such as login credentials, from eavesdropping. The easiest way to tell if your site has SSL is to look for a padlock in your browser's address bar -- that means you're browsing the site securely!
- Content Private/Public
    - Take a moment to review your site's content security settings. This determines who can access your files, library documents, calendar events, and other content on your site.
- Passwords
    - Strong passwords are key to keeping your site safe and secure. All passwords should be required to contain at least 1 upper case letter, 1 lower case letter, 1 number and be between 8 and 15 characters long, and should be updated regularly.

While we know speed and convenience may make it so security is not always at the forefront of everyone's thoughts, during this already trying time we want to make sure that we are all doing everything we can. We will continue to

educate and inform our clients of any other scamming techniques in order to keep your club safe.

1-800-352-6647
support@jonasclub.com
sales@jonasclub.com