MembersFirst®

Clubs Are Being Targeted By Scammers

During this time, more than ever, it's critical to continue to be vigilant about your club's cybersecurity. Unfortunately, scammers take advantage of people during a time like this because our compassion levels are escalated and our focus is scattered.

It has come to our attention that some clubs and their members have recently been the target of email scammers. Scammers are targeting clubs to gather information then creating a Spoofing or 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).

When used together, these attacks are very powerful. For example, a scammer could request money from a member using a fake club staff email address, or a scammer could use a fake club staff email address to request member information from another staff member. It is very difficult to spot these fake email addresses at-a-glance. They are typically one letter or one number different from a real email address or have a different TLD (.org vs .com) and the "from name" will be a real staff member's name.

What you 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 whom you are sending the information.
- Use file-sharing tools such as Dropbox, Google Drive or SharePoint to pass sensitive internal documents to one another. It helps with not only security but operation challenges such as version controls and access.

At MembersFirst, we take security very seriously by investing heavily in proper infrastructure and resources while constantly monitoring our systems. However, the 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 cybersecurity.

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! You can learn more about SSL in our Learning Center. If you are interested in adding SSL to your site, click here to get started.

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. By default, all new files are marked Private Only which means only logged in members may view the file. If you want to allow public users to view the file you must either choose Public Only or Public and Private.

Warning: Do not make any files containing sensitive information Public or Public/Private. Public files can be accessed and cached even if you do not link the file anywhere on the site. You can always change the security setting of a file later by following these instructions.

Passwords

Strong passwords are key to keeping your site safe and secure. All passwords are required to contain at least 1 upper case letter, 1 lower case letter, 1 number and be between 8 and 15 characters long. To gain full credit on your site's security dashboard, your password reset interval needs to be 180 days or fewer to foil any attempt by brute force attacks. Given enough time and computational power, all attempts to access any system via brute force will succeed if passwords are not changed regularly or otherwise locked out. Please contact your Client Services Manager to discuss your club's current universal password parameters and discuss all options.

Lockout Users

If someone tries to log in to your member's account too many times, the system can automatically lock the member's account so they cannot gain access to your site. More often than not, this is caused by members forgetting their own passwords, but it is better to be safe than sorry. If an account is locked, the member will see an error instructing them to contact the Club. To unlock the account, edit the member's profile in the member directory and click "Delete" next to the red "Locked Out" status. We recommend locking accounts after five failed login attempts to help keep your site secure. Contact your Client Services Manager if you would like to enable this on your website.

Security Score

We give everyone a "report card" for your site's security. Your site's security score is displayed prominently on the admin side, within the header and is an indicator of how well your site implements these additional security measures. Some measures, such as adding SSL, are more effective than others in keeping your data safe. We recommend reviewing your site's security dashboard from time to time to keep your score as high as it can be. Following the advice in the email will surely boost your score —and your website's security!

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.

Thank you for being a great customer of MembersFirst.

Stay safe out there!

Kevin Baer
Director of Operations
(508) 310-2304
kbaer@membersfirst.com