

NOTICE TO MEMBERS



Notification of Cyber Intrusion to Club Servers

Dear Member,

As we informed you in our letter dated 20th August 2020, the Club was targeted by a cyberattack detected on 3rd August 2020. On that day, the Club's IT systems were subject to a ransomware attack, during which files on a number of our servers were encrypted. The Club took immediate steps to recover the vast majority of the data from backup servers and to block the ransomware from continuing to operate.

The Club immediately contacted cybersecurity experts and engaged a leading cyber forensic company, Kroll, to undertake a full investigation starting the day after the Club became aware of the attack. We also filed reports about the incident with law enforcement agencies including the Hong Kong Police.

It was important to us to notify members of this incident before the forensic investigation had concluded so that precautionary steps could be taken to protect personal data. We also arranged access to identity protection services at no cost, which we offered to members in our communication dated 25th August 2020.

Since that time, we have continued to proactively liaise with law enforcement and relevant international authorities, including the Hong Kong Privacy Commissioner for Personal Data.

With the investigation now concluded, we wanted to provide you with a final update and bring your attention to additional relevant findings, actions the Club is taking, and outline the precautionary measures that have been recommended for you.

The Final Report

Our cybersecurity experts found that the attack began on 29th July 2020 and managed to access our systems on 1st August 2020 after several unsuccessful attempts.

The investigation found no conclusive evidence that member data was exported from our systems or that data on the core membership server was accessed. However, it concluded that some basic member data including names, contact details (email addresses and phone numbers), dates of birth, and Hong Kong ID numbers of Club members and family members was affected and at risk of being extracted.

The investigation also found no conclusive evidence that other member data may have been at risk. Importantly, the investigation confirmed that there was **no evidence** that any financial member data (i.e. bank or credit card details) was either accessed, extracted or within the data that was at risk.

NOTICE TO MEMBERS



Notification of Cyber Intrusion to Club Servers

Out of an abundance of caution, we are encouraging all members to take steps to safeguard themselves. Please see “Recommended Precautionary Measures” below for more information.

Actions the Club is Taking

We take cybersecurity seriously.

In line with guidance from law enforcement agencies, the Club has not paid, and does not intend to pay, any ransom.

We have continuously invested in infrastructure to protect our systems from cyber-attacks. Although there is no way to entirely guard against threats of this nature, the Club is dedicated to seeking expert advice on how we can further enhance our cybersecurity resilience.

In their final report, the cybersecurity experts outlined a number of recommended steps for the Club to take, on top of the steps already implemented by the Club, to improve the overall security of the organisation. All these recommendations have been considered by the Club and are being implemented where appropriate. These include:

- Improvements to firewalls and additional restrictions on remote access
- Upgrades to PCs and servers to further guard against potential vulnerabilities
- Enhanced security monitoring/ testing of network devices and endpoints
- Additional end-user/ staff education on latest cybersecurity threats

Recommended Precautionary Measures

To help you monitor your personal information for certain signs of potential identity theft, the Club continues to offer you a complimentary 12-month membership to Experian IdentityWorksSM. This is now available for sign up on or before 15th December 2020.

As explained in our communication dated 25th August 2020, the service monitors the web, social networks, and public databases on your behalf 24/7. It looks for your details to immediately detect theft, loss, or disclosure of your vital personal information and financial information (although your financial information is not currently thought to have been at risk in the intrusion). If your information is found, you will be instantly alerted and given help and advice on what to do next to protect yourself from fraud.

We encourage you to take up this offer, as it is in line with best practices for those who may have been affected by a cyber intrusion. If you wish to use this service or have any questions about the intrusion, please contact the Club on idmonitor@hkfc.com for an activation code.

NOTICE TO MEMBERS



Notification of Cyber Intrusion to Club Servers

In addition, we recommend that you take the precautionary actions described in our original communication dated 20th August 2020, namely:

- Monitor accounts that use personal data;
- Change the login credentials for online accounts, including but not limited to those used to access Club facilities and online members' area;
- Use strong passwords and change them regularly. Try to keep password at least eight characters long and use numbers, upper case, lower case and symbols;
- Enable two-factor authentication on all your online services where possible;
- Be suspicious if anyone contacts you by email, phone call or text message asking you to confirm your personal details. Never give out personal details unless you're sure who you're speaking or writing to; and
- Check your bank and credit card statements regularly for any unusual payments that you don't recognise.

Conclusion

We will continue to work with our cybersecurity experts to implement their recommendations and to take appropriate follow up actions related to this incident.

I fully understand and appreciate your concern regarding this matter and I apologise once again for any inconvenience this may have caused you. We hope that the above provides you with comfort that we take these matters seriously, have taken prompt and efficient action once we discovered the intrusion to resolve this matter and to proactively protect you, and will continue to enhance our IT security in line with expert recommendations.

If you have any questions about this matter, please contact the Club at cyberenquiries@hkfc.com.

Yours Sincerely,

Michael J Wood
Chairman
Hong Kong Football Club