Payment Diversion Fraud Alert – February 2020

NHS CFA have issued an Intelligence Bulletin (IBURN-2020-02-01) which is an update to previous alerts we have issued in recent months relating to reports of payment diversion frauds, where staff members are targeted by fraudsters for their salary payments, often via the ESR system.

Reminder: The staff member receives an email with a false incentive such as logging into ESR to accept a pay rise. The email contains a link to a website which appears the same as the NHS ESR log in page. The fake page allows the fraudster to collect the staff member's username and password. From here the fraudster can access the staff member's ESR account and change the bank account details, along with other contact and personal details which may enable further frauds beyond the NHS.

The Met Police (Cyber Team), NHS National Investigation Service, National ESR team, NHS Digital and financial institution counter fraud teams are still investigating the ESR Salary Diversion Fraud and considering future prevention methods. This bulletin has been updated to include a couple of more examples of potential phishing emails sent on the 6/2/2020.

Example Fraud Email 1
This notice is to inform all employee & staff of the current general upgrade of our server. This upgrade would help the organization to offer all eligible staff & employee their benefits, promotion and increment. All staff are hereby directed to re-validate their details in order to effect the new salary payment plan and increase in salary for the month of February through the New Year 2020. Kindly click on the link NEWPAY to re-validate your payment information and also apply for salary increment and promotion. We sincerely apologize for all inconveniences that this may cause you.

Example Fraud Email 2
All staff and Employee are expected to verify their Data for the Month of February salary and staff benefits payment, Please kindly Click SecurePayroll and complete the required directive, failure to comply with this directive will lead to omission of payment

Actions:

- Staff should remain vigilant at all times to these types of emails.
- Be alert to potentially spoofed email addresses and web addresses, along with poor spelling and grammar, as well as any emails or links requesting your personal or login details to be entered.
- If staff have any concerns about emails of this type that they have received, or responded to, they should contact their Anti-Fraud Specialist as a priority.

To view previous fraud information alerts sent out, please visit the fraud section of the CCG's website.

Kevin Howells
Anti Fraud Specialist

Telephone: **07825732629** / **0161 743 2008**
Email: kevin.howells@miaa.nhs.uk / kevin.howells1@nhs.net