**Beware of Mandate Fraud**

Mandate Fraud is a fairly common tactic which is often used by cyber criminals.

In these cases, a fraudster impersonates a known and trusted supplier. They may spend time “grooming” the victim, by entering into a series of emails or phone calls to try and build rapport.

Eventually, the fake supplier will ask for the genuine company’s bank details to be updated. When this is actioned, invoice payments which were due to be paid to the supplier are then diverted into the fraudster’s bank account. Often, the first the victim knows about this is when the real supplier gets in touch to chase up the missing payment.

Mandate fraudsters are increasingly sophisticated, and will steal information from various sources to make themselves look and sound more legitimate.

Common signs of a mandate fraudster include:

* Contact is often by email from an email address which looks similar to the supplier’s real email address. Small changes might be made such as adding in an extra letter or piece of punctuation.
* Sometimes, the fraudster will use a hijacked a genuine email address which is being used by the supplier. Emails will be sent from the account without the supplier being aware.
* Mandate fraudsters may make it look as though they have copied in other known contacts at the supplier or NHS organisation. Often, this is done by using fake email addresses which impersonate other people that you may know and trust.
* Contact details quoted on the persons email signature may be missing or altered.

What you can do to avoid mandate fraud:

* Always confirm requests for bank details or contact information to be changed by contacting the supplier directly, and using their official contact information (never rely on contact details which have been provided within emails)
* Look out for slight changes to email addresses or phone numbers.
* If you think you have been targeted and have sent a payment to the wrong place, contact your bank immediately to see if they can stop the payment. Make sure you have the fraudster’s bank details to hand as the recipient bank may also be able to help.
* Never be embarrassed to double check requests.