


UN3652 1 of 3 21 <sup>st</sup> August 2025	Electronic Staff Record Programme USER NOTICE	
<b>Title</b>	Self Service Account Security Reminder	
<b>Purpose</b>	Reminder of steps to take to protect Self Service Accounts	
<b>Intended Audience</b>	All ESR Users	

## SUBJECT

This notice is intended for all ESR Leads, local IT Departments, and, where relevant, to be shared with NHS employees that access ESR to remind of steps that can be taken to protect Self Service Users and their ESR accounts.

Despite security being embedded within the design of ESR, Self Service Users are still at risk from phishing incidents.

It is likely that IT Departments at Employing Organisations have already issued advice on good practice relating to emails to their employees, so this User Notice is intended to complement or supplement that advice.


## DETAIL

### What is Phishing?

Phishing is usually an attempt to deceive the recipient of the email into thinking a legitimate organisation is requesting information from them. These requests for information may look innocent at first glance or may seem to come from a legitimate source, but do not. These scams indicate that the recipient must reply to an email, respond to a request by phone, or follow a link to a web site.

### What might a Phishing e-mail look like?

- **Links that appear to be ESR links but they are not.** If the recipient places their cursor over a link in a suspicious email, the email program most likely shows you the destination URL. It is important not to click the link but look closely at the URL. A URL that is formatted `esr.fakewebsite.com` is taking you to a location on `fakewebsite.com`. Just because “esr” is part of the URL does not guarantee that the site is an official ESR website.
- **Requests for personal information.** Official ESR emails will **never ask** the recipient to reply in an email with any personal information such as a National Insurance number, Date of Birth or Employee Number.
- **Urgent appeals.** ESR will **never claim** that an account may be closed if the recipient fails to confirm, verify or authenticate their personal information via email.
- **Messages about system and security updates.** ESR will **never claim the need to confirm important user login/account information** via email due to system upgrades.
- **Obvious typing errors and other errors.** These are often the mark of fraudulent emails and websites. Be on the lookout for typing or grammatical errors, awkward writing and poor design.

UN3652 2 of 3 21 <sup>st</sup> August 2025	Electronic Staff Record Programme USER NOTICE	
<b>Title</b>	Self Service Account Security Reminder	
<b>Purpose</b>	Reminder of steps to take to protect Self Service Accounts	
<b>Intended Audience</b>	All ESR Users	

## ACTION REQUIRED

All Organisations are asked to roll out Multi Factor Authentication to reduce risks;

### What are the benefits of MFA?

- Keeps your personal data in a more protected environment.
- Helps you gain access to your account should you forget your password.
- Provides increased protection against cyber attacks, including social engineering attacks
- Checks if an attempt is made to access your account from an unusual location or device.

### The NHS employee should :-

- never send passwords, employee numbers, or other private information in an e-mail.
- be wary of any unexpected e-mail attachments or links, even from people they know.
- when logged into ESR in their browser, look for 'https://' and a lock icon in the address bar before entering any private information. The ESR Self Service website shows the lock icon and "IBM United Kingdom Limited".
- have an updated anti-virus program running on the device in use, that scans e-mails.

ESR has additional protection, specifically for Bank Account Changes, whereby an email is initiated to the email address held for the employee. It is imperative that, should an employee receive an email advising that their bank account details have been amended in ESR, they check this email for it's validity.

### What to do if an NHS employee using ESR Self Service falls victim to a phishing scam?

- Ensure that this is raised with their local ESR Team as a matter of urgency
- Immediately ask the User to change their password.
- Report the incident to the ESR Support Team via the ESR Service Desk.
- Check all personal details.

## FURTHER INFORMATION

We refer you to the National Cyber Security Centre guidance (link below) where there is excellent advice about what to do if you think your employee may have been hacked.

National Cyber Security Centre - <https://www.ncsc.gov.uk/section/respond-recover/you>

## NEXT UPDATE

None