MHR

The Payroll Pirates: Are your staff salaries safe?

Cybersecurity

Get started

The science behind
a new world of work

The latest threat to your payroll and how to protect yourself

Will North, CISO, MHR International UK Ltd

A new cyber threat has been identified using sophisticated techniques to gain unauthorised access to HR systems and steal staff salaries.

The cyber security company Silent Push recently published research into a new threat group they are calling “Payroll Pirates.” The group are using sophisticated methods to trick staff into handing over their HR system username and password, then logging in as them and changing the bank account where their salary is paid into.

Anatomy of an attack

The Payroll Pirates have been observed creating fake login pages of organisations' real HR systems. These look identical to the legitimate login pages, apart from a slightly different URL. For example, using a different top level domain such as ".online" instead of ".com".

To get staff to visit their fake sites, the group purchases ads with well-known search engines to get their fake sites at the top of search results. This technique is successful as staff often navigate to their HR system by typing the name into a search engine and clicking on the top link, rather than going to a saved bookmark as you might expect.

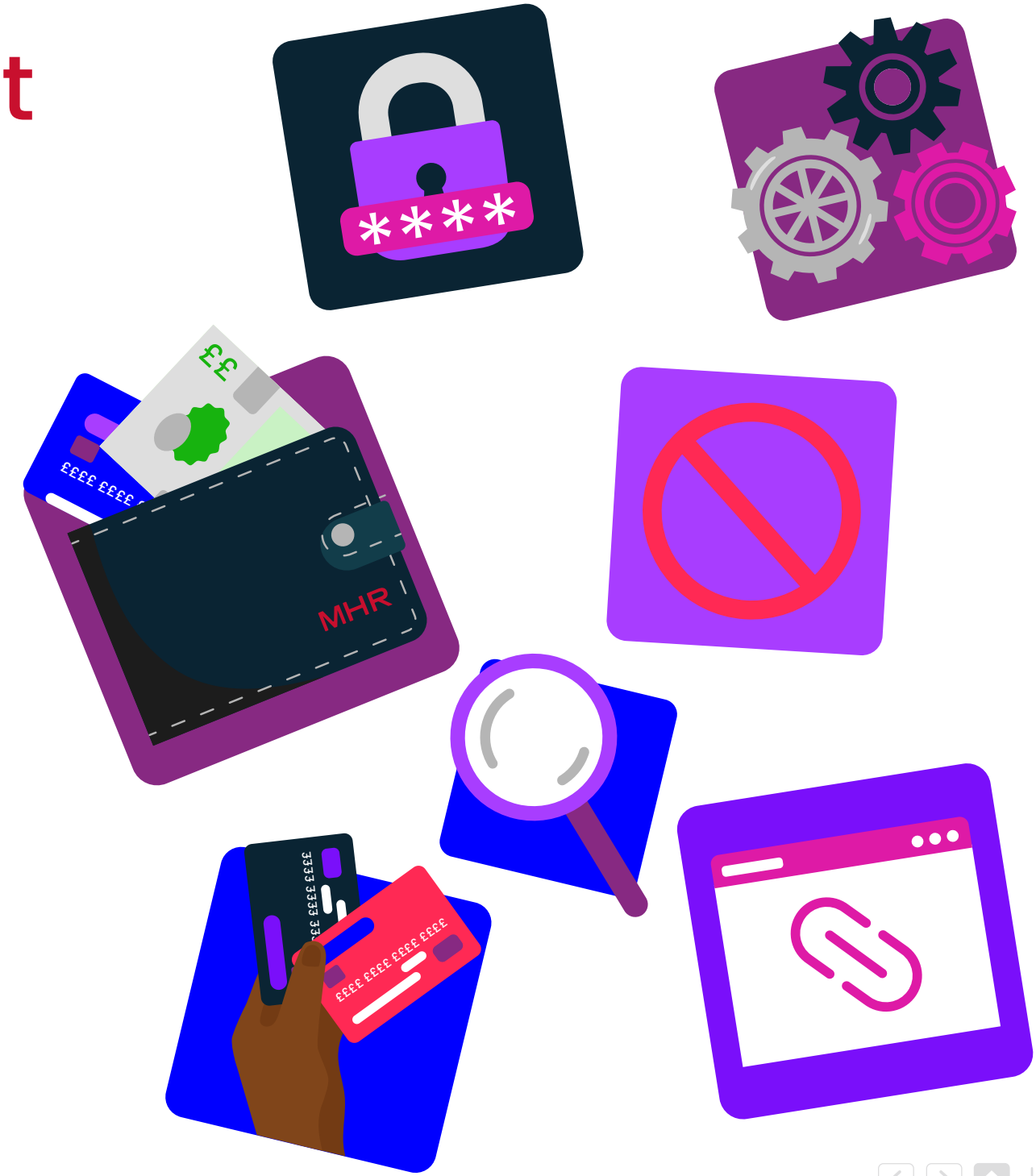
Once the member of staff logs in to the fake website, their username and password is captured and used by the group to login to the real HR system. The bank account details of the employee are then changed to redirect funds to a fraudulent bank account, which the threat actors control. This process is typically automated.

Organisations only know they've been attacked once a member of staff contacts HR to say they have not been paid.

How to protect yourself

Although this is a relatively sophisticated attack, there are many things organisations can do to protect themselves.

- **User training** – train staff to use bookmarks for important websites rather than navigating to them via search engines, and to check the URL is as expected when entering sensitive data into a webpage
- **Links to HR systems** – don't include links to your HR systems on publicly accessible websites to make it harder for attackers to find
- **Multi-Factor Authentication (MFA)** – use MFA for accessing sensitive systems so that a stolen username and password alone is not enough to login. Use FIDO2 certified MFA where possible
- **Bank account notifications** – configure your HR system to send alerts to both the user and HR when a user changes their bank account, so that it can be verified
- **User Behaviour Analytics** – monitor and block suspicious activity such as users changing bank account details from previously not used IP addresses



How is MHR protecting customers

MHR provides multiple security solutions within its products to protect against these types of attacks. A stolen username and password will never be enough to log in. With additional security hygine measures like using strong passwords and protecting physical devices, you should be more than equipped to handle this latest threat.

For MHR customers, MFA is included as standard for all our solutions. To find out more, visit our cyber security hub or get in touch with your Account Manager.

Your next steps

People First is an HR, payroll and finance platform that helps you achieve everything outlined in this guide and more. If you're looking for a system that supports and elevates your M&A strategy to ensure a smooth transition for everyone, then it ticks every box.

Want to learn more about how it works?

Contact us >

info@mhrglobal.com | mhrglobal.com | +44 (0) 115 945 6000 (UK) | +353 (01) 541 3778 (IRE) | +1 (470) 890 6170 (US)

1671- Payroll Pirates - Whitepaper - v1_02_25