Going Back to the Office? You're a Perfect Target for Phishers

If you, like millions, are mulling a return to the physical office after a year working from home, be warned. Criminals have been exploiting people's fear and curiosity regarding the COVID-19 pandemic from the very start, and experts say this is sure to continue as long as the virus affects our private and professional lives.

Phishing attacks have continually exploited public interest in COVID-19 relief, variants, and vaccines by spoofing the Centers for Disease Control, the IRS, the Department of Health and Human Services, the World Health Organization, and others.

New attacks

Now, according to researchers at security firm Inky, employees returning to work in offices and other company premises can expect cyber crooks to impersonate their colleagues and company executives. Judging by earlier campaigns, attackers will hit you with emails made to look like they're coming from HR, or possibly from the CEO.

Lures will likely include:

- Phony surveys regarding workers' willingness to receive a vaccine.
- Alleged new internal precautionary measures, supposedly to support health and safety.
- Information about changes in rules and new security roles within the company.
- Requirements to review new policies.

What you can do

- If your employer is beginning to move workers back to company premises, be extremely vigilant with notification emails you receive. Remember, spearphishing messages may look completely legitimate, with company logos and actual (spoofed) return addresses.
- Don't let any email cause you to perform an action that feels wrong, such as transferring company funds or divulging your password.
- Use the phone to confirm any email requests that strike you as unusual or "not quite right."