DigiKnow
CYBER SECURITY DEPENDS ON YOU

PROMPT BOMBING AND
My.Delaware.gov

July 2022 | Issue 2022:6

TIME IS RUNNING OUT!

Digital government services are rapidly expanding in the State of Delaware. Offering secure access to an individual with a proven identity via a single sign-on solution for citizens and constituents is key to enabling people to easily make purchases and transact personal business with multiple state agencies.

The need to harden the State of Delaware network against cyber threats has never been more critical. The majority of employees in the Executive Branch have secured their access.

If you are a state employee and want to continue to view your paycheck and benefits online, it's imperative that you register for my.delaware.gov NOW! After June 30, 2022, this will be the only way to access your information.

The link below will take you directly to the registration information. In five minutes, you will be on your way to safe secure access. Additionally, you will be helping to create better digital government experiences for all Delawareans.

https://youtu.be/4-Qm-b9edho

For more information:

My.Delaware.gov - Employee Self Service's New Home - Department of Technology & Information (DTI) - State of Delaware

Remember, TIME IS RUNNING OUT, REGISTER NOW!

Not Your Ordinary Bomb Threat

Multifactor Authentication - is a security technology that allows software to verify the identity of a user's log-in request by using something they have like a mobile device or a part of the body like a fingerprint or an eye scan. The State's MFA technology supports the use of test/SMS, voice calls, an authenticator app for smartphones or a hardware token.

Even with organizations using the latest in MFA technologies, the bad guys continue to try to find their way around it. One of the ways they explore holes in a system is called: **prompt bombing. It** is an attack that has been around for a while and is not very complicated. The goal of prompt bombing is to gain access to an account or service that leverages MFA by sending as many MFA approval requests as possible to a user at an inopportune time in hopes that the user is distracted enough or irritated enough, they will unknowingly give the attacker access. An attacker might spam a user with requests in the early morning in hopes that the user will authorize the request allowing the user to go back to sleep.

My.delaware.gov is the solution offering identity and access management for Delaware’s many digital government endeavors. Delaware seeks to offer a highly personalized experience to anyone with a relationship to state government. Anyone doing business with Delaware government can have a single, validated identity for secure transactions conducted for a variety of purposes, across many agencies.

My.delaware.gov comes with an advanced version of multi-factor login called Adaptive-MFA. This means my.delaware.gov only questions a login when risk threats call for it. This could be if you try to access a sensitive application, you connect from a high- risk country or location, or when you login from a new device. my.delaware.gov will go live for the State's employee self-service and Pension applications in August 2022 to further harden our employees' information.

Not only does my.delaware.gov provide a secure single sign-on for digital government services and information it also provides alerts when someone logs in from a different computer. This includes the location of the login event.

Should you become the target of a prompt bombing attack, resist the urge to make the approval requests just "go away." Report the attack to your system administrator and immediately reset your password. If you are the administrator, now is the time to force password resets and start checking logs. DTI employs risk visibility and controls teams to research and balance risk with the controls needed to address it.

Information sourced from: WIRED, NIST, NephoSec