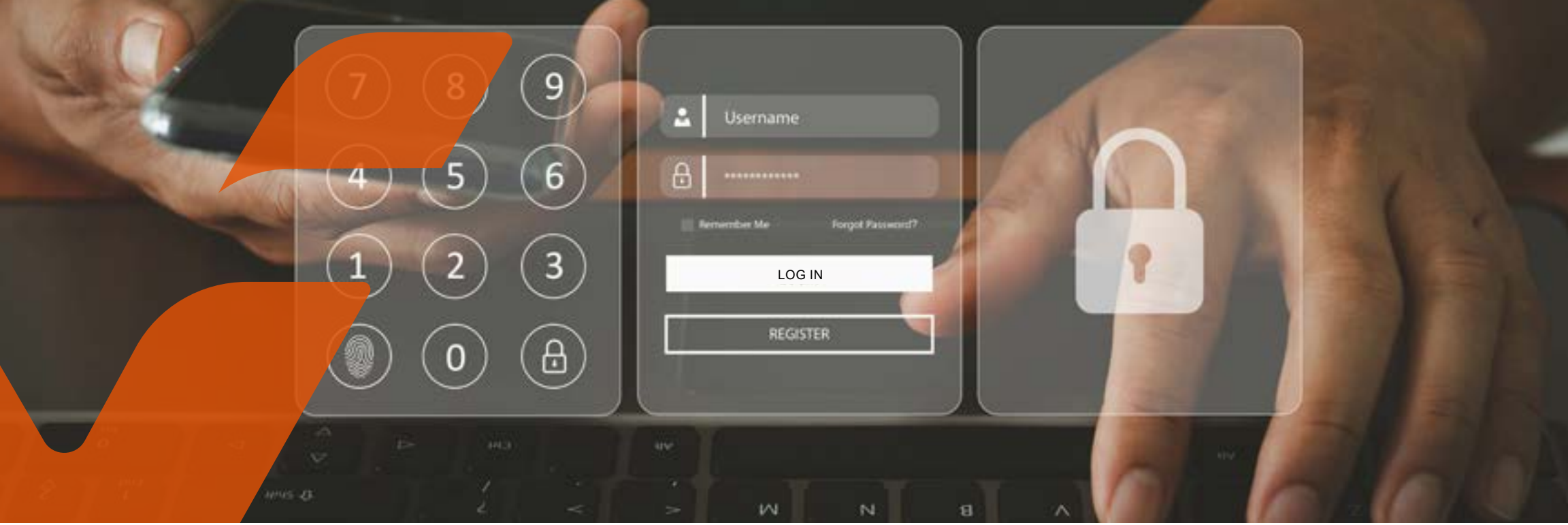

Cyber tips: Multi-factor authentication

VICTOR

Multi-factor authentication (MFA) demands extra verification factors to make sure a user is who they say they are. The tips below provide insight into why MFA is vital for security in today's threat landscape, considerations for implementing it and further resources to help get it set up.

What is multi-factor authentication?

MFA is a security mechanism that requires two or more methods of authentication to verify the identity of a user attempting to gain access to a computer resource, such as an email account or admin account on a server. Multi-factor authentication combines two or more factors: something the user knows (such as a password or passphrase), something the user has (a security token) and what the user is (a biometric verification such as fingerprint or facial recognition).

Why is it important?

MFA is extremely important due to the increasing sophistication of cyberattacks. MFA can help stop malicious cybercriminals from accessing your data or that of your company. Even if your password is in the hands of a cybercriminal, it is unlikely that they will have your other forms of verification too.

Even if your password is in the hands of a cybercriminal, it is unlikely that they will have your other forms of verification too. This is what makes MFA so important.

When should I use MFA?

- Companies — Where possible, MFA functionality should always be enabled for all staff when they are using server-related software, externally accessed applications such as Microsoft Office 365 or Google Workspace or other similar applications.
- Individuals — Where possible, individuals are advised to activate MFA when accessing websites that require the submission or access to financial information, when submitting sensitive personal information or when accessing email accounts.

Where can I use it?

You can use MFA with any website or application that has enabled its functionality. Microsoft has enabled MFA for use with its applications and websites as have Google and other tech companies.

How do I implement it?

MFA can be implemented in a number of ways depending on the type of security token or other verification factor that is chosen for authentication. However, implementing MFA requires some careful thought and planning, especially for larger organizations.

Considerations include:

- Being clear about what you want to protect
- Understanding the MFA technology that you will use
- Understanding the impact on employees and making them aware of MFA

When rolling out MFA, it is advisable to begin with your most important accounts, such as admin accounts. These are the high value targets cybercriminals wish to target as they can use these accounts to pivot through the organization. After these, roll out MFA to privileged users in key business roles or to those that have access to important or sensitive business communications.

Completing the following will make for a successful rollout of MFA:

- Have an inventory of systems and applications. Knowing what you have will allow to identify priority systems.
- Prioritize systems according to the criticality and sensitivity of the data being accessed.
- Have an onboarding process for staff and for software applications.
- Test how applications work with MFA prior to deployment.

Further information

- Government of Canada — Canadian Centre for Cyber Security
  - › Secure your accounts and devices with multi-factor authentication
- Learning resource about MFA for business using Microsoft can be found here.
- For a tutorial on how to enable MFA in Microsoft Azure click here.
- Instructions on how to set up MFA in Microsoft Office 365 can be found here.
- An MFA roll out pack containing customizable posters and email templates for businesses can be found here.
- An MFA setup guide for Google Workspace can be found here.
- Victor cyber resources
  - › Victor Cyber insurance
  - › Guide: "Cyber liability exposures: How to protect yourself and your business from a cyberattack"
  - › Guide: "Cybersecurity: Work securely from home"
  - › Infographic: "Cyberattacks: A threat to all businesses"
  - › Video: "A day in the life of a business owner in a cyberworld"
  - › Video: "Victor experts share preventative measures as cyberattacks on the rise"

#TheThreatIsReal

Visit us at victorinsurance.ca/cyber.