SECURING DEVICES AT HOME & WORK

The three basics of securing your accounts are:

using a strong password,
updating your devices, and
adding Multi-factor Authentication to your accounts.

What may be new to some in the previous list is Multifactor Authentication (MFA). In a recent newsletter, the OXEN Technology News group gives a great overview. This flyer contains portions of their blog.

You may have noticed that recently a lot of your accounts, both personal and work, are now requiring multiple methods of verifying your identity when you login. No longer do you just enter your username and password to get into your email, your cloud apps, or your accounting system. You now also need to input a short code that is texted to you, generated by an app, or emailed. In some cases, you might be getting verification phone calls, using a smart card, or entering biometric data like a fingerprint.

Why is multi-factor authentication a big deal?

MFA can stop many common brute force attacks and phishing attempts. All it takes is a hacker to compromise a single email account in your organization. Suddenly coworkers start receiving legitimate-looking emails from a person they trust asking for sensitive information. Then the entire organization can be compromised. But by enabling MFA, email accounts on services like Office 365 are much more secure and difficult to hack. (In 2019, Microsoft started rolling out mandatory multi-factor authentication in Office 365 to certain organizations and partner accounts. They know how essential MFA is, and they're going to make it a default.)

The reality is that many traditional cybersecurity measures can be compromised without MFA. Anti-virus software, firewalls, encryption tools, network monitoring solutions, and more can all be bypassed if hackers compromise them and gain credentials to privileged user accounts. MFA is a beautifully simple solution to lock down accounts even further. And it's often not that hard to roll out either.

What is MFA?

MFA consist of three things that when combined verify someone's identity.

This is often summarized as:
something you know,
something you have, and
something you are

Example of all three: a combination of username, password, codes, tokens, and/or biometrics.

MFA may seem like hassle, especially when you're setting up these multiple verification methods, or if you need to run to find your cell phone for that text message code.

But it's making your accounts more secure by requiring multiple pieces of information or identification from you. This lessens the likelihood that someone will have all the pieces of data they need to hack an account. A hacker may have your username and a list of your commonly used passwords, but if they don't have the third or fourth verification steps, they'll be stopped in their tracks. And this is a very good reason to not be afraid of using MFA!

Reasons MFA is important

So, what are some quick reasons why multi-factor authentication is so important?

1. Identity theft is easy, and it's a growing threat to all businesses. MFA makes identity theft harder.
2. Weak or stolen credentials are a hackers' go-to method in a majority of attacks. MFA beefs up the strength of credentials considerably. It also makes stolen passwords less fruitful for hackers.
3. Small businesses are being targeted at a growing rate by cyber attackers. New security measures are not for enterprise-class organizations only. MFA is simple and relatively easy for small organizations to roll out.
4. Other cybersecurity tools and solutions, like anti-virus and firewalls, are only as strong as their user authentication procedures. MFA can make your existing perimeter security stronger.
5. High-ranking employees and highly privileged user accounts are a hot target for hackers. MFA can be used specifically for administrative and executive accounts to protect them.
6. Cybercrime is about more than just stealing data. With MFA, you're also attempting to stop attackers from destroying data, changing programs, and using your accounts to transmit propaganda, spam, or malicious code.
7. MFA is already becoming ubiquitous. People are accustomed to authentication procedures in their personal as well as professional lives. Social media, banking, gaming, and email platforms have all rapidly adopted MFA. Bringing it into your workplace is a no-brainer.

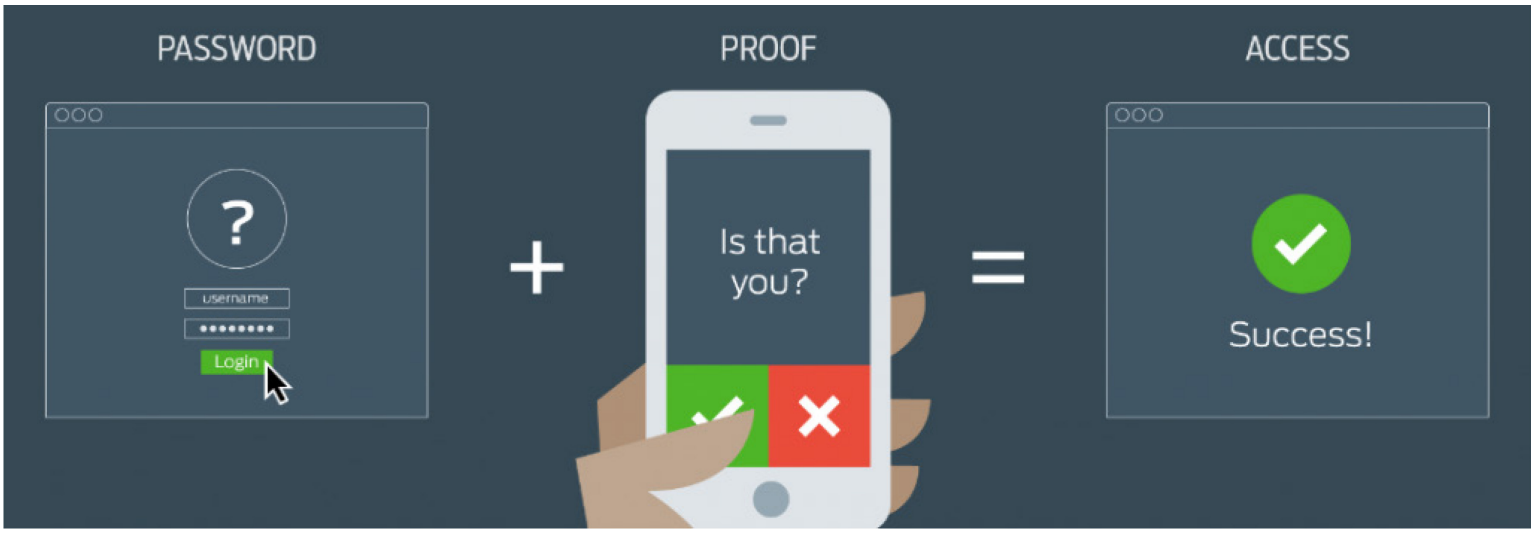
FAST FACTS

Multifactor Authentication (MFA) - No longer is a username and password enough security. Whenever you have the ability to add MFA, do so.

Keep A Clean Machine- Keep your devices updated. Updates are given b/c vulnerabilities have been discovered with your device and the updates "patch" these vulnerabilities. Don't let our devices become like a leaky boat!

Passwords- You hear this every year. Why? A weak password or repeated password used on multiple accounts is a huge vulnerability.

Keep Tabs on your Apps- Your apps could be using default permissions you never realized you approved. Check your app permissions.



Need to report a security issue?

The Department of Innovation & Technology (DoIT) is committed to protecting our customers. If you have found a vulnerability or security issue, we ask that you submit a detailed description of the issue to us at: DoIT.Security@illinois.gov.