SMALL BUSINESS BIG THREAT

Small Business, Big Threat

Quickly Tips for Staying Safe Online

There are a few things you can do to help protect yourself and your employees.

Password Etiquette

The password has been around for a long time, and it's still our first line of defense. When coming up with a password to use, it's important that you **DON'T**:

- Use personal information as part of your password
- Store your password on a post-it note near your computer
- Use the same password for multiple accounts
- Share your password with ANYONE

Please **DO** follow these best practices when creating passwords:

- Use a long phrase instead of a complex password:
    a. EXAMPLE: TheDetroitLionsRock123 instead of d3tr0it
- Use different passwords for different accounts
- Utilize a password manager for tracking multiple passwords.

Find the "S" in HTTPS

All secure websites and services such as online banking will be using a secure browsing session using the HTTPS protocol. You can verify this when browsing by looking at the address bar and looking for the HTTPS at the beginning of the URL. This insures that any information sent over this connection is protected by SSL encryption. Example: **https**://www.google.com/

Beware of unknown senders in e-mail

It is recommended that unless you know the sender of are expecting a specific piece of e-mail, that you don't open it. Many viruses find their way into PCs everywhere via carefully crafted e-mail messages. While spam filtering is an option, there is no way to stop 100% of spam messages, so user training and knowledge is extremely helpful in this situation.

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

If it doesn't feel right, it probably isn't

Common sense goes a long way when trying to protect yourself online. If something looks too good to be true, or something doesn't look right, simply stay aware from it. If you run across something that you need to access, but don't know if it's safe, contact your IT services provider for further assistance in assessing the potential threat.

Don't browse sensitive information on public Wi-Fi

Public Wi-Fi is just that, PUBLIC. Anyone can hop on it and use the network. This means potential attackers as well. It's very common for attackers to be "sniffing" for information on these public networks to see if they can gather any personal information. Therefore it's highly recommended that any personal or business information not be accessed while on these networks.

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation