CAROLINA CYBER NETWORK

Developing Talent | Protecting Our Future

31 DAYS OF CYBERSECURITY

31 small steps to help make your business more cyber secure.

01 Take a few minutes to think about what information would hurt your business the most if it was lost or stolen.

02 Make sure your phone and computer are protected with a PIN, password, or fingerprint/Face ID.

03 Check your devices for any software updates you've been putting off.

04 Turn on multifactor authentication (MFA) for your email.

05 Check your other important accounts and turn on MFA anywhere it's available.

06 Back up the files you couldn't afford to lose.

07 Test your backup by restoring a file. A backup only helps if it actually works!

08 Look through your user accounts. Does everyone still need the access they have?

09 Remove any accounts that belong to former employees.

10 Take a look at what devices are connected to your network. Do you recognize all of them?

11 Check your router, printer, cameras, and other devices for default passwords that were never changed.

12 Find one password you've reused and change it to something unique.

13 If you aren't already using a password manager, take a few minutes to look into one.

14 Turn on automatic updates so you don't have to remember to do them yourself.

15 Run a security or antivirus scan on your computer.

16 Look through the programs on your computer and uninstall anything you no longer use.

17 Brush up on the warning signs of a phishing email.

18 Find an example of a phishing email and see how many red flags you can spot.

19 Make sure everyone on your team knows what to do if they receive a suspicious email.

20 Check your shared files and folders. Is anything being shared with someone who no longer needs it?

21 Take a look at your business Wi-Fi settings and make sure your network is secured.

22 Check your Wi-Fi password. If it's weak or has been shared with too many people, it might be time for a new one.

23 Check your important accounts for any logins or activity you don't recognize.

24 Think about the sensitive information your business keeps and where it's stored.

25 Ask yourself: Who would I call first if we had a cybersecurity incident today? Write it down.

26 Make a simple plan for what your team should do if an account gets hacked, a device is lost, or something just doesn't look right.

27 Spend a few minutes learning about a cybersecurity threat that businesses are dealing with right now.

28 Talk to your team about cybersecurity. Ask them what security issue worries them the most.

29 Look over your cybersecurity policies. Is anything outdated or missing?

30 Pick three cybersecurity things your business could realistically improve next.

31 Look back at everything you did this month and keep it going. Small changes can make a big difference!