Franklin County
BOARD OF COMMISSIONERS
1803

Protecting Yourself Against Cybercrime, It's everyone's job to look out for themselves and others.

Dear Residents, Employees, Elected Officials, Community Partners, and Businesses,

Given recent events, we recognize the need to take proactive measures to protect our community. This is an opportune time to educate residents about cybersecurity, equipping everyone with the knowledge to safeguard their personal information and stay alert to potential threats.

In our rapidly evolving digital landscape, defending yourself against cybercrime is more crucial than ever. As your County Commissioners, we are committed to ensuring you have the resources and tools to protect your personal information and maintain online safety.

Here are some essential tips to help you stay secure:

General ways to protect yourself from potential scams that may result in identity theft:

- Do not give out your personal information unsolicited over the phone, email or by text.
- Report as Junk and Delete texts from numbers you don't recognize.
- Do not reply to emails that ask you for money and do not click on links in emails you don't recognize.
- Use different passwords for your different personal accounts and change them on a regular basis.
- Monitor your bank and credit card statements for unauthorized use, and if you see anything, notify your bank, law enforcement and the credit bureaus.

Some additional precautions to consider:

1. Create Strong, Unique Passwords

    - Use Complex Combinations: Mix uppercase and lowercase letters, numbers, and symbols.
    - Avoid Reuse: Each account should have a distinct password.
    - Consider a Password Manager: These tools help generate and store secure passwords.

Commissioners
Kevin L. Boyce, President
John O'Grady
Erica C.Crawley

373 S. High St. 26th Fl.
Columbus, Ohio 43215

t_ 614 525 3322
f_ 614 525 5999

2. Enable Multi-Factor Authentication (MFA)

- Add Extra Security: Multi-Factor Authentication requires an additional verification step beyond your password, such as a code sent to your phone.
- Activate for Key Accounts: Focus on email, banking, social media accounts, and any password keepers you may use.

3. Be Cautious with Emails and Links

- Verify Senders: Do not open emails or attachments from unfamiliar or suspicious sources.
- Check Links: Hover over links to confirm they lead to legitimate sites before clicking.

4. Be Aware of Social Engineering

- Protect Personal Information: Be cautious about sharing personal details online or over the phone.
- Verify Identities: If contacted by someone claiming to be from a trusted organization, verify their identity through official channels.

5. Backup Your Data Regularly

- Keep Copies Safe: Use an external drive or secure cloud service to back up important files.
- Test Restorations: Ensure you can access and restore your backups when needed.

6. Practice Safe Browsing

- Use Secure Websites: Only enter sensitive information on sites with HTTPS encryption.
- Avoid Public Wi-Fi for Sensitive Transactions: If using public Wi-Fi, consider a Virtual Private Network (VPN) for added security.

7. Keep Your Software Updated

- Install Updates Promptly: Updates often include critical security patches.
- Use Automatic Updates: Where possible, enable automatic updates for your software and apps.

8. Protect Your Wi-Fi Network

- Change Default Passwords: Use strong, unique passwords for your router.
- Enable Encryption: Use WPA3 or WPA2 encryption to secure your network.
- Use a Guest Network: Set up a separate network for visitors to keep your main network secure.

9. Educate Yourself and Others

- Stay Informed: Keep up with the latest cybersecurity news and best practices.
- Share Knowledge: Help family, friends, and neighbors understand these practices to enhance community safety.

Your safety and security are our top priorities. By following these guidelines, you can reduce the risk of falling victim to cybercrime. For additional resources or assistance, you may want to obtain a free copy of your credit report by visiting www.annualcreditreport.com, or calling 1-877-322-8228. If you would like to take an additional precautionary measure, you may want to freeze your credit report with all three credit bureaus.

- Equifax 1-800-349-9960 or www.equifax.com
- Experian 888-397-3742 or www.experian.com
- TransUnion 888-909-8872 or www.transuion.com

Stay safe and secure!

Presented on the behalf of the Franklin County Board of Commissioners

Sincerely,
Kenneth N. Willson, MPA, CTA, ECI
County Administrator