DATA SECURITY TIPS

PROTECTING YOUR DATA

KOSS OLINGER

Invested in You

Information security is more important now than ever before.

We hope that these tips will help you take control and better protect your devices, accounts, and personal data.

BEWARE OF SCAMS & PHISHING ATTEMPTS-KNOW THE RED FLAGS

USE UNIQUE, STRONG PASSWORDS FOR EVERY ACCOUNT

USE A PASSWORD MANAGER

LOCK YOUR PHONE & DEVICES

CREATE ONLINE ACCOUNTS BEFORE IMPERSONATORS DO

USE TWO-FACTOR & MULTIFACTOR AUTHENTICATION

MONITOR DATA BREACHES & CHECK TO SEE IF YOUR INFO HAS BEEN COMPROMISED

PRACTICE OTHER GOOD DIGITAL HYGIENE HABITS

2700-A NW 43rd Street, Gainesville, FL 32606, (352) 373-3337 or 1-800-373-3302. Securities offered through ValMark Securities, Inc. Member FINRA/SIPC. Advisory Services offered through Koss Olinger Consulting, LLC. An SEC Registered Investment Advisor. Koss Olinger and ValMark are separate entities.

DATA SECURITY TIPS
PROTECTING YOUR DATA

KOSS OLINGER
Invested in You

BEWARE OF SCAMS & PHISHING ATTEMPTS – KNOW THE RED FLAGS

Scams and phishing attempts now look very believable. To help identify if something may be a scam, be on the look-out for these red flags:

- Information or an offer that's too good to be true.
- Quick timeframe for providing requested information.
- Unable to talk in person to verify their identity.
- Emails, texts, or phone calls seeking personal information, including passwords.
- Sender email addresses that do not match the company an email is supposedly being sent from.

USE UNIQUE, STRONG PASSWORDS FOR EVERY ACCOUNT

Your password is your first line of defense against unauthorized access to your accounts. Some tips for stronger passwords include:

- Use a different password for each of your online accounts. If one service provider gets compromised, hackers try to use the same credentials on other sites.
- The longer your password, the better. A good rule of thumb is a minimum length of 10 characters. Aim for 12-15 characters or use a short phrase.
- Don't use familiar people, places or things in in passwords.
- Keep your passwords confidential and secure.

USE A PASSWORD MANAGER

Password managers are highly recommended by security experts to protect your credentials from hackers. They help ensure that each website has a unique and hard to guess password.

- Write down the "master password" for your password manager and store it in a safe place that only you have access to, like a safe or lock box.
- Do not use and disable the password keeper in your browser.
- Choose a reputable password manager. Password manager services to consider:

LastPass	https://www.lastpass.com
1 Password	https://1password.com
Dashlane	https://www.dashlane.com

LOCK YOUR PHONE & DEVICES

Your devices hold a wealth of personal information!

- Protect your phone with a lock screen.
- Lock your computer or iPad when you walk away from it.
- Use fingerprint or face scan technology unlock options

CREATE YOUR ONLINE ACCOUNTS BEFORE IMPERSONATORS DO

Even if you prefer paper statements, setting up online accounts prevents others from "claiming" them. Examples of accounts to set up are banking, credit cards, loans, 401(k)s, investment accounts, etc.

- Check your online accounts monthly to make sure all information is accurate and up to date, including your email and street addresses.
- Sign up for email and/or text alerts that notify you of changes or transactions.
- Use multifactor authentication.

USE TWO-FACTOR & MULTIFACTOR AUTHENTICATION

Add two-factor authentication (2FA) or Multifactor authentication (MFA) wherever possible.

- 2FA and MFA requires another piece of information to verify yourself, such as a text message, security question, or use of an authenticator app.
- Helps to prevent unauthorized users from gaining access to an account with only a stolen password.

MONITOR DATA BREACHES & CHECK IF YOUR INFO HAS BEEN COMPROMISED

While there are bad guys out there actively trying to compromise data, thankfully there are also good guys monitoring and alerting the public of data breaches. Below are a couple of reliable sources:

- **Have i been pwned?** https://haveibeenpwned.com/
  Website created by a Microsoft employee and well-known security expert. A free resource to quickly assess if you may be at risk due to an online account having been compromised or "pwned" in a data breach.
- **Firefox** https://monitor.firefox.com/breaches/
  The Monitor from Firefox lists websites involved in breaches (Breaches tab) and allows you to enter your email to see if you've been part of a data breach (Home tab)

PRACTICE OTHER GOOD DIGITAL HYGIENE HABITS

Other tips for good digital hygiene include:

- Avoid public Wi-Fi if possible. If on public Wi-Fi, do not log into personal accounts or use passwords.
- Use anti-virus protection on your devices.
- Promptly install software and app updates.
- Never click on emails or texts seeking personal information, including passwords.