Aldridge Consulting
WE HELP YOUR BUSINESS GROW

6 CYBERSECURITY TIPS

OCTOBER IS CYBERSECURITY MONTH

If you run a small business, you may think that hackers won't target you, but the truth is you're likely more vulnerable to cyberattacks. Data from 2019 showed that small businesses were the target of 43 percent of the data breaches in 2019. Hackers view small businesses as easy prey because they believe their security is easier to bypass than larger corporations. The easiest, no-cost step you can take is to ensure all computer systems and applications are kept up to date with the latest upgrades and patches. Here are six more steps you can take to protect your accounts and your data.

1. GET THE SOFTWARE

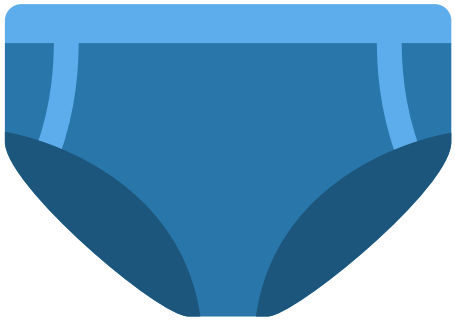
Download and install reputable antivirus and anti-malware software on all your devices and be sure to enable automatic updates. The software can identify, quarantine, delete and report any suspicious activity. This also prevents hackers from using malware installed via phishing emails or other methods to steal your usernames and passwords or to remotely access your computer.

2, BE AWARE OF SOCIAL ENGINEERING SCAMS

Scammers will sometimes pretend to be IT or security personnel from well-known companies and request remote access to your computer or ask you to disclose a password under the guise of fixing some non-existent issue on your device. Unless you have initiated contact with someone, do not grant access or give them your passwords.

3. PASSWORDS ARE LIKE UNDERWEAR

Change them often, don't share them and don't leave them lying around. Always use unique usernames and passwords for each of your accounts. Scammers purchase compromised login details from the dark web and test them on various websites to find people who reuse credentials for multiple accounts. Password manager apps will allow you to use a different password for every site without having to remember each one.



4. ENABLE TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) should be enabled on all your accounts. This requires you to type in a one-time code that you receive on your mobile phone. 2FA acts as an extra hurdle for hackers, even if they find out your username and password.

5. ADD EXTRA SECURITY OFFERED BY YOUR MOBILE SERVICE PROVIDER.

Many mobile phone carriers offer features to prevent scammers from porting your phone number to a new device and attempting to use your phone number to access account information.

6. BACK UP YOUR INFO.

If you suffer a ransomware attack, a good backup will save the day. Whether online (cloud), offline (external drive) or both, just do it. Use automatic backup software to set a backup schedule, and don't store your external hard drive next to your computer – in case of theft, fire, or flood.

BOOKKEEPING
CONSULTING
PAYROLL

30 years experience as a Chief Financial Officer & accounting professional

WHAT WE DO

- Business Consulting
- Process Improvement
- Staff Evaluation
- Financial Reporting
- Budgeting & Forecasting
- Bookkeeping Cleanup
- Account Reconciliation
- Payroll Services

WHO WE ARE

Certified QuickBooks Pro Advisors with experience in the service, real estate, transportation, restaurant, construction trade sectors and more!

CALL FOR A FREE CONSULTATION (928) 224-0527

Aldridge Consulting
WE HELP YOUR BUSINESS GROW

Cindy Aldridge
PO Box 2288 Lake Havasu City, AZ 86405
(928) 224-0527 | cindy@aldridgeconsultingllc.com