Part 3 of a 3 Part Series

ARE YOU CYBER SECURE?

Tips to help you answer "Yes!"

Follow these tips to see how cyber aware you are and decide what you can do to improve your agency

AWARENESS

Make cybersecurity a conversation at staff meetings. Set clear expectations for staff to protect personally identifiable information (PII). Update your processes and procedures to reflect the importance of cybersecurity for your agency and your customers.

PLANNING

Institute a breach response plan as part of your disaster recovery plan.
Try these:
Data Breach Response: A Guide for Business
Data Security Breach Notification Sample Letter | Department of State
ACT - Disaster Guide

USE VPN

Use a Virtual Private Network (VPN) when on public W-Fi , working from home, at the airport, or hanging out at the coffee shop.

CULTURE

Have regular conversations with your staff about the importance/risk of a cyber breach for your agency - a risk avoidance culture is a powerful way to minimize the chances of a breach.

INSIDER THREATS

Insider threats are real!
Establish clear and swift procedures for deprovisioning terminated employees, notifying carriers, collecting agency property, and identifying who in your organization needs to know.

REMOTE WORK

Establish and enforce protocols for work-from-home employees to protect your customers' personal information.
Try these:
ACT's Remote Work Guide
2022 Data Breach Investigations Report | Verizon

SOCIAL ENGINEERING

According to Homepage | CISA, More than 90% of successful cyber-attacks start with a phishing email - a trick designed by bad actors to have you reveal your passwords, social security number, credit card numbers, or other sensitive information. Think before you click.
Red Flags Warn of Social Engineering (knowbe4.com)

BIG i® AGENTS COUNCIL FOR TECHNOLOGY®

independentagent.com/ACT