CYBERSECURITY TIPS FOR ALASKANS

What is Cybersecurity?

Cybersecurity is the art of protecting your personal information and electronic devices from access and use by criminals. Good cybersecurity practices will ensure that your information and devices remain easily available to you while making it difficult to access for attackers.

Always be vigilant—it only takes one mistake to give criminals access to your information.

What are the most common threats?

- **Phishing:** Criminals create emails, texts, and malicious websites that pretend to be from organizations you trust (banks, charity organizations, online shopping sites, the Social Security office, and more) to steal your personal information, like your credit card numbers and login details. These are often paired with fake "urgent" messages or demands.

- **Scams:** Be wary of ads or messages offering "free" gifts or prizes. These are tricks designed to get you to give up personal information to steal your personal information or money.

- **Malware:** When you download a malicious program (also known as malware), your computer can be damaged and the personal information it contains destroyed or stolen. Criminals and attackers do this to make money by selling your personal information, like your credit card information or tax forms.

How can I stay safe online?

Online scams and phishing that target older people are happening more and more. The internet may seem like a dangerous place for seniors targeted in phishing attacks, but it doesn't need to be with the next page's simple steps (flip page). →

Phishing Attacks: Don’t Get Hooked

1. **Think before you click:** If you receive an unexpected or demanding email, message, or text, take a moment to calm down before clicking. Criminals use powerful emotions like shock and fear to get you to click and enter personal information before thinking twice.
2. **Use Google, not email or text, to get to a website:** Whenever possible, don’t click email or text links. Accessing a website through your favorite search engine will avoid fake websites set up in phishing attacks and allow you to confirm the message is real.
3. **It’s OK to call the organization:** If you have followed steps 1 and 2 and don’t see the message, call the organization using the contact information on its real website. If they don’t know what you’re talking about, the message is likely a phishing attempt.
4. **Trust your gut:** If you receive an offer that seems too good to be true, it probably is! Be especially warry of any offers of free prizes in exchange for your personal information.

Staying Safe Online:

1. **Find the lock:** When entering personal information, verify the website is secure by finding the lock (or the letters https://) next to the website address bar. This ensures your information will be securely transmitted, but does not by itself guarantee the website is real.
2. **Use Strong Passwords:** Use passwords that are long (10-16 characters), unique, and do not contain personal information. If a website provides the option, also turn on Two-Factor authentication to receive a one-time code on your email or phone each time you try to log in.
3. **Update your Software:** Don’t delay. If you see a software update notification, act promptly, or turn on automatic updates if you can. Updates contain important and timely security fixes.

What to do if I am a victim of an attack?

1. **Change your password:** Changing your password to something unique and different as fast as possible will prevent your information or accounts being stolen. Accounts with similar passwords should also be changed as soon as possible.
2. **Call for help:** .
    a. **Fraud:** If you or someone you know has been a victim of elder fraud, help is standing by at the National Elder Fraud Hotline at 833—FRAUD—11 (833—372—8311), available from 6 a.m. to 2 p.m. AKST Monday-Friday. This is a free, U.S. Department of Justice-run callcenter to help report fraud against anyone age 60 or older.
    b. **Identity Theft:** If you or someone you know has had a criminal steal your personal information to commit fraud (such as apply for credit, file taxes, or get medical services), visit identitytheft.gov or call 877-438-4338 for a recovery plan.