Tips For

Laptops, Tablets or Mobile Devices

Security

The recent trend toward remote work has required many state employees to use our state-issued laptops or tablets outside of the office or at home with increasing frequency. These security tips are therefore a timely resource for state employees for both information access and physical security of these devices. Moving these devices between home and office locations can leave them more vulnerable to theft or loss.

Physically protecting laptop computers from theft often involves common-sense measures. These devices should be treated as though they were cash. Just as you would not leave a few thousand dollars in cash on the seat of your car, or on the bed in a hotel room, you should not leave these devices lying around. They need to be treated as the valuable items they are. More important than the worth of the device is the information stored on them.

There are some basic but important steps to protect the files and data contained on these mobile devices. First, the device should be protected by password and two-factor authentication, if possible, and any data contained should be encrypted to West Virginia Office of Technology encryption standards. Also, never connect to a public or insecure Wi-Fi connection for the access and transmittal of data and use the state's virtual private network when accessing the state's network. Be very cautious of potential phishing emails or scams on these devices. One wrong click can open the contents of these devices to hackers. Protecting access to the data contained on the laptop will mitigate the risk of disclosure should the device be lost or stolen. In addition to protecting the files contained, there are methods to physically protect the device itself from theft.

Below is a list of safeguarding suggestions for these devices. These suggestions should be communicated to your employees with proper documentation of training/communication.

<u>Laptop Safeguarding Suggestions:</u>

1. Thieves can identify laptops by their carrying case. If practical, carry the laptop in a nondescript case, such as a briefcase, that does not identify it as a computer;

2. When carrying a laptop in its case walk with your hand directly on the bag strap, with the computer slightly in front of you. This makes it difficult for "snatch and grab" attackers who attempt to slip the case of your shoulder while racing in the other direction;

3. Do not ask a stranger to watch your laptop while you make a phone call, go to the restroom, throw something away, or get something to eat. Thieves are everywhere and can look very businesslike and trustworthy;

4. Avoid leaving the laptop in an unattended vehicle. If you must leave it in a vehicle, lock it in the trunk. However, don't wait until you get to your destination to lock it in the trunk since someone may be watching;

5. Place the laptop in front of you or on the counter while conducting transactions at a hotel, airline, or car rental desk;

6. Never check laptops as luggage. If stolen, they may be damaged by rough handling;

7. If you are using your laptop for a presentation, do not leave it in the presentation room overnight or when you go to lunch;

8. In your hotel room, use a hotel safe if provided with one to protect your laptop. If a safe is not provided and you must leave it in your room, do not advertise its presence-put it and the carrying case in your luggage or in a drawer; otherwise take it with you.

Document by:
Jeremy C. Wolfe
Risk & Insurance Manager
and
Ashley Summitt
State Chief Privacy Officer
WV Board of Risk and Insurance Management

References:
ISO Services Properties, INC- 2003. Silverplume