Working From Home? Here Are Five Security Tips

The PIA Partnership Program—Winning@Cybersecurity Defense* (pianational.org/cybersecurity)—*helps educate your agency about cybersecurity.

Working from home has been an adjustment for everyone. Many of us have not only shifted our work environments, but we also have to make sure we're working securely. In your agency's office, you are operating on a secure network that has firewalls to prevent hackers from getting in. But at home, you and your devices are more vulnerable–and bad actors are aware of it. *Ransomware has grown 600% since 2015 and nearly half of all organizations have been hit.*

Here are five ways to avoid an attack when you're working from home:

1. **Be on alert for phishing scams that seek to infiltrate your computer**

Phishing scams are one of the most common forms of attack. These can come via email or text asking you to open a tainted attachment or click a virus-laden link or via phone asking you to divulge personal information. Hackers have also gotten very good at making these messages appear like they are coming from legit sources.

Top items to watch out for include:

- Generic language, such as Mr. or Ms., Sir or Madame
- Bad grammar, language, or punctuation
- A sense of urgency
- Requests for sensitive information, especially via email or text

Keep a reminder of these warning signs by your computer. If you ever are unsure if an email is legit, before clicking a link or opening an attachment double check. Find an actual person from the organization that supposedly sent the message and confirm that they did in fact send the note. If you do uncover a scam email, let others at your agency know so they can be on the lookout.

2. **Separate work devices from personal devices**

Keep your work devices and personal devices separate. Ask your agency if they will provide you with a phone to use while at home. A number of agencies us VoIP (Voice over Internet Protocol) which allows you to receive calls no matter where you are. These systems usually come with designated phones. For more information on VoIP services visit Winning@Virtual (pianational.org/winningatvirtual)

Make sure your work computer is only used for work. Don't allow your kids to use it for schoolwork. Any leisurely internet browsing, online shopping or social media activity should be done on personal devices.

3. **Avoid public Wi-Fi.**

If you need a change of scenery and want to go down to the local coffee shop to do some work, don't log onto the public Wi-Fi. These networks are unsecure and data shared on them can be accessed by others. If operating outside of your home or agency office, use your phone as a personal hotspot – but make sure it has a strong password and select WPA2 network security.

4. **Update your devices.**
   Don’t ignore software updates on your computer or your smartphone. As software developers uncover security flaws in their programs, they create patches to fix them which they deliver to users via system updates. Whenever a device prompts you to update, accept them. If you are in the middle of something and aren’t able to do the update immediately, reschedule it for that evening. Most updates will give you an option to postpone.

5. **Make sure video conferences are secure.**

We have all become so comfortable with videoconferences, and they are great ways to maintain face-to-face interactions when being remote. But these can also be susceptible to hackers. For example, during the pandemic, *Zoombombing*, became a trend, as uninvited participants found ways to access and disrupt meetings.

Require participants to enter a password to enter a meeting. If your program has a waiting room capability activate it, so the host has the final say in who is allowed to pa

.