Someone creating a tremendous sense of urgency, often through fear, important deadline.

Pressure to bypass or ignore security policies or procedures, or an offer too good to be true (no, you did not win the lottery!).

A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.

One of our goals is to enable you to work as securely as possible from home. Below are five simple steps to working securely. The best part is all of these steps not only help secure your work, but they will make you and your family far more safe as you create a cybersecure home.

First and foremost, technology alone cannot fully protect you - you are the best defense. Attackers have learned that the easiest way to get what they want is to target you, rather than the technology. (If they want your password, work data or control of your computer, they’ll attempt to trick you into giving it to them, often by creating a sense of urgency. For example, they can call you pretending to be your bank, utility or other company, or send you an email warning that a device on your network is infected. Or perhaps they send you an email warning that a package could not be delivered, fooling you into clicking on a malicious link. The most common indications of a social engineering attack include:

- Someone creating a tremendous sense of urgency, often through intimidation, a crisis or an imminent deadline.
- Pressure to bypass or ignore security policies or procedures, or an offer too good to be true (no, you did not win the lottery!).
- A message from a friend or co-worker in which the signature, tone of voice or wording does not sound like them.

Ultimately, the best defense against these attacks is you.