# FAQ for End Users

Below you will find a variety of questions that you will likely encounter from your end users. Some of these questions will not be directly answered in this document as they are driven by your unique policies and integration. However, we have supplied suggested best practices and insight on how to answer these questions.

1. What is a YubiKey?
   A YubiKey is a compact and extremely robust hardware security key that stops account takeovers. It is both faster and easier to use than existing legacy solutions.
   ***You may want to personalize this response with some additional verbiage on why your organization selected the YubiKey to provide secure authentication.***

2. What happens if I lose my YubiKey?
   ***This will largely be determined by your internal policy and procedures.*** *However, the recommended best practice for Yubico customers is to ensure that each user has a spare key. We have them for our most valuable assets in life – our houses, our cars, our PO and safety deposit boxes, etc. and Yubico encourages you to do the same for your digital devices.*
   *A spare key will enable your employees to securely authenticate with the exact same security level instead of downgrading it with less secure authentication methods, and it will enable the user to work without having to call the helpdesk support, guaranteeing productivity and decreasing money spent on supporting a user who is not able to authenticate.*

3. Does the YubiKey read my fingerprint when I touch it?
   *Only with the YubiKey Bio Series. For all others, the touch sensor on the YubiKey only detects capacitive touch and is not biometric. By requiring the user to touch the YubiKey to login it is verified that the person logging in is a real live human behind the computer, and not a remote hacker, bot, or malware.*

4. Does it require batteries?
   *It requires no battery or cellular network connectivity. The YubiKey is crush-resistant and water-resistant. It is manufactured domestically in California and Sweden.*

5. Does the YubiKey use Bluetooth (BLE) to communicate with my devices?
   *No, the YubiKey uses the secure NFC communication protocol. BLE does not provide the security assurance levels of NFC and USB, and requires batteries and pairing that create a poor user experience.*

6. Will I need to change my PIN as frequently as my password? **(if applicable to your integration)**

*No. your selected PIN is stored securely on the YubiKey and is never transmitted to any remote services where it could be intercepted so you will not be required to change your PIN as you would with your password.*

7. Can I use my YubiKey for personal accounts?
   ***This is determined by your organization's policy.*** *However, encouraging users to leverage their YubiKey for business and personal accounts will reinforce good habits. Additionally, if a hacker is unsuccessful in targeting specific employees in their place of business, they will most likely attempt to compromise their personal accounts.*
   *Since there are no shared secrets across services/applications, privacy and security is maintained, thus there is no risk in using the YubiKey for both. If the user leaves the organization, access can be revoked, so users can no longer access internal resources.*

8. Can the YubiKey be used as a USB storage device?
   *The YubiKey has no functionality as a mass storage device and is recognized by the computer as an HID (Human Interface Device, similar to a keyboard). The YubiKey is designed to only be a user authentication or identification device.*