I have two perspectives on this, one is mine and one is a family member's. Mine first, here's what happens every time I sign into Amazon.com:

- Amazon fires the "create passkey" browser API, without explaining what's happening. They just do it immediately after I finish authenticating.
- My password manager intercepts the API and prompts me to save the passkey. Usually I cancel it, but let's imagine I did want to make a passkey.
    - Saving passkeys in a software password manager seems risky to me, so I press the button to pass the request through to my OS.
- Now Windows asks whether I want to create the passkey using a phone/tablet/etc. or using a USB token. I have a USB security key, so I choose that one.
- Now Windows tells me to insert my USB key. At this point several things can happen. I may be prompted for my key's PIN, I may not. I may get a "this will let example.com see the make and model of your security key" warning, I may not. The website may choose to create a "resident key", or a "non-resident key". If the site creates a resident key, it will permanently use up one of the "slots" on my USB key since there's no way to manage or delete them other than wiping the whole thing. As a user I often won't feel confident whether or not that happened, because neither the site nor Windows will make that clear.
- Once the key is added, I have no idea how it will impact the security of my account. In Amazon's case I think they'd just use it as an additional sign-in method while still allowing the other ones. For some sites I might prefer to specifically require one of my security keys, but almost no one provides that as an option and generally it's hard to tell what is or isn't considered sufficient for authentication or recovery without testing it.
- I have to manually label my keys “A”, “B”, “C”, etc. with a sharpie and then enter those same names on each website (if allowed) because there’s nothing unique about them and no way to set a persistent name on the key itself.

Now here's the thing, I don't even know if any of that is "passkeys". Is it only a passkey if I use a mobile device? Only if it’s a resident key? All I know is I find it really confusing, and I have a CS degree! I like the idea of using my security keys for things, but I'm constantly afraid that I'll fill up the storage since I can't even tell if a site is going to make a resident key or not. And it’s hard to keep track of which keys have been added to which accounts unless I make some sort of spreadsheet. Some sites only allow me to add one key, or allow multiple but don’t let me name them.

Now for a more "normal user" perspective, using a phone. My aunt recently asked me to help her go through some of her online accounts and make sure she had all her security settings up-to-date. At one point she asked me about passkeys, something she's seen mentioned on websites but never used (to her knowledge anyway). I did my best to explain it to her, and we basically concluded that it's not worth it for her at the moment because it's too confusing and potentially risky. Some points of confusion:

- She has an iPhone and a Windows desktop. I think in theory there's a way to store passkeys on a desktop directly (maybe you need a Windows Hello camera?) but I don't really know how that works. Even if we could do it, she would end up with two passkeys (one on the phone and one on the desktop) and would have to manage them independently. However if she had a Mac, it would be two copies of the same passkey, since they sync through iCloud. This creates an odd situation for websites since they can't really label a specific passkey as "your iPhone 14" (since it could be used on any Apple device), but it's totally possible to have multiple distinct passkeys and need to tell them apart (for instance to delete an old one).
- If she creates one on her phone, she'll only be able to use it if the desktop has Bluetooth (idk if it does). If she's at someone else's house or on vacation or whatever, she'll only be able to use it if the computer she encounters happens to also have Bluetooth working, right? Will creating a passkey stop her from using other methods to sign in? If not then they don’t really protect her from phishing, right?
- Once a passkey is created, how do you manage them? I think it’s a little better on iOS, but I at some point created a passkey for CVS on my Android phone and it’s very difficult to “find” it. When I sign into CVS.com on a desktop I’m not even given the option to use a passkey, and once I’m signed in I can’t find anything in my account settings to show or delete the passkey. But if I sign in on my phone, I’m prompted for my fingerprint right away, so it is working. I was eventually able to find a list of my stored passkeys on my phone by searching in the settings app for “password” (not “passkey”, that doesn’t go to the right place) and opening the Google Play Services Password Manager, an interface I’ve never seen before and I doubt I’ll remember how to find again. My aunt would be hopelessly confused by this I think.
- If her iPhone is lost or stolen, what happens? In theory the passkeys are backed up to her Apple account, but when she signs into iCloud she has to verify by responding to a prompt on her phone, so it’s not clear to her how she’d even get back into iCloud. If someone steals her phone after seeing her PIN, can they use her passkeys? If so she doesn’t want to use it (she doesn’t store her regular passwords on her phone because of this concern).