What's Next

As computing power increases and cyber threats multiply,
we'll see big changes...some very soon, others down the road.

The end of passwords

> The average employee has 191 passwords, and 80% of breaches are the result of stolen passwords. Your phone's biometrics — particularly face scans — will replace passwords, allowing you to more securely access email, bank accounts, websites, and apps.

More control of your personal information

> Apple is about to give users more choices in how apps like Facebook and WhatsApp treat their personal information. And Congress may eventually enact privacy laws similar to those in Europe that allow anyone to be "forgotten" by search engines.

Streaming video crackdown

> This year, another 27% of cable TV users will switch to streaming apps like Netflix and HBO Max. Those networks aren't profitable yet, so some streaming networks will merge and raise rates, and most will follow Netflix, which has announced a crackdown on users who share passwords.

Smarter watches, earbuds, and glasses

> Smartwatches and earbuds will add important functionality, monitoring blood sugar, sleep patterns, blood pressure, and heart health. New computerized eyeglasses will display turn-by-turn directions and view information about nearby restaurants and stores as you move.

5G wireless begins to deliver

> Super-fast wireless internet will allow vehicles to communicate, adjusting to approaching traffic conditions, and reducing the number of auto accidents. 5G will also replace your home Wi-Fi, securely tying together smart appliances and apps, allowing you to work from home more securely.

Massive computing power comes home

> "Quantum computing," with computers that deliver far more power than today's home PCs, will eventually deliver supercomputing to the home. The size of hard drives will also increase dramatically: a Japanese company has unveiled an 80 terabyte drive, which is enough to store four million hours of movies.

The rise of "zero trust"

> Many organizations will use technology to limit the types of websites, apps, files, and emails that employees can access online. This "zero trust" approach is a response to today's fastest-growing cybersecurity problem: ransomware, where crooks lock computers and networks so the owners can't access information. A ransomware attack occurs every 14 seconds.

REGIONS

Sources: FORBES, LIFEHACK, WEARABLE, INFOGUARD, SYMANTEC, CM ALLIANCE, GOVTECH, WIRED