**Ways Hacking Will Evolve in the Future**

**Proposed Methodologies**

When it comes to the future of hacking the expression, “You ain’t seen nothing yet!," is very appropriate. Despite all your security measures, from your extra firewalls, double and triple authentications al la RSA, anti-virus programs, and paper shredders to your SecureID keyfobs and cards, hackers are prevailing.

The future of hacking, like the future of technology, is always squirming and breeding and morphing just beyond the normal person’s line of sight.

## HACKERS MIGHT BE ABLE TO BREACH YOUR DATA BY TOUCH ALONE.

Don’t think a hacker needs a computer and an internet connection to take an invasive look at your data. At some point, chips implanted under the criminal’s skin might be able to prompt a phone to open a link—possibly under the guise of a security update—that could lead to a malicious site. All a hacker would have to do is be near the device or hold the device in their hand. If this threat increases, we could see a rise in the use of blockers that protect devices from being compromised. Your purse or wallet, for example, would be shielded from such attacks.

1.**Dark Knight Attacks**- From Microsoft Kinect to smart phones, everything is connected to the Internet and comes equipped with microphones, video cameras, gyroscopic feedback, and GPS. “In the movie The Dark Knight, they hacked into every cell phone to build a live three dimensional image of everything happening within Gotham City,” explained Harry Sverdlove, CTO of Bit9. “The technology to do this is within reach today. Through facial recognition, speech pattern identification, and geo-location feedback, future hackers could raise ‘targeted attacks’ to a new level."

## HACKERS WILL USE OUR EYES TO DECEIVE US – BIO HACKING

“Newer biometric authentication systems will replace passwords, quite possibly with a mix of ocular and filial credentials,” said Kurt Baumgartner, senior security researcher at Kaspersky Lab. “Whatever the credential replacement is, we will see cyber criminals respond with devices that parallel ATM skimmers of today. Iris skimmers and spyware that steals identification information provided by [a person's] eyes will be implemented and distributed.”

1. **RAM scraping**- “For years everyone has been locking down databases since they are the source of information, but now hackers that can breach a server can get an application less than 1MB in size on the server and capture all the data as it is written to RAM before it goes to a database,” said Chris Drake, CEO of FireHost. “An application like this can also capture data (such as credit card numbers) that don't even go into a database, but that are processed by a third party provider. RAM scraping will be a huge concern as it gains more popularity among the hacker crowd."

## HACKERS MIGHT JOIN YOUR EMAIL CONVERSATIONS.

Many of us laugh at the clunky, transparent email attempts to lure us into malicious website links, and email services do a good job of diverting suspicious correspondence to a junk folder. But hackers may one day be able to mimic legitimate exchanges so well that they can drop a message in the middle of an existing email thread. Because it will blend seamlessly into the dialogue, the danger of giving up confidential information will grow exponentially—which is why it’s important to never share sensitive information via email, no matter who you’re communicating with.

## HACKERS MIGHT TAKE OVER OUR ASSISTANCE ROBOTS.

Today, smart homes are all about voice recognition and app-controlled environmental regulation: Think about asking your television to change the channel or telling your thermostat to warm up the living room before you get home. But as we move into an era of locomoting robots that provide home assistance—cleaning, dispensing information, or surveillance—consider that hackers could hijack their sensory inputs to eavesdrop on sensitive conversations and relate personal information. Consumers will likely need to be proactive by turning off information-gathering options that are on devices and staying on top of possible breaches reported in media.

## THEY’LL USE YOUR COMPUTER TO DO THEIR DIRTY WORK FOR THEM.

Not all financially-motivated hacking is devoted to separating you from your money. Sometimes, hackers just want your computing power. Cryptojacking is expected to rise in the coming years, with criminals luring people to websites that allow them to harvest your computing power to generate, or “mine,” cryptocurrency (which it does by solving complex math problems). While you may not suffer as a direct result, it’s still a pretty egregious use of your property to pursue a criminal act—and you’re not likely to even notice. Never click on suspicious links and make sure anti-spyware software is up to date.

**Note:**

1. **The sub points under each bullet point are names of methods which have already been worked out by someone.These need to be included in the presentation.**
2. **Please don’t add bulk of lines altogether,instead add 2 or 3 lines in one slide and divide the rest into more slides.**
3. **Try to make the presentation look minimal and interactive so that the audience won’t get bored..**