**BLUEJACKING**

**by**

**ADINGIJIR KENAS SATI**

**st/cs/nd/19/051**

**BEING A SEMINAR PAPER**

**PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY,**

**FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**DECEMBER, 2021**

**Abstract**

*Bluejacking is probably the most common form of Bluetooth hacking. This happens when a hacker searches for discoverable devices in the area and then sends spam in the form of text messages to the devices. This form of hacking is rather childish and harmless. It was once used mainly to prank people in the past when mobile devices came with Bluetooth that was automatically set to discoverable. Bluejacking is used today for spam messaging and the hackers who use this do it just to frustrate others. The method does not give hackers access to your phone or the information on it. Bluejacking involves Bluetooth users sending messages to other Bluetooth users within range. Although sensitive information may not be revealed, unwanted messages may show up on your device.*

## INTRODUCTION

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e. for bluedating or bluechat) to another Bluetooth enabled device via the OBEX protocol. Bluetooth has a very limited range; usually around 10 meters on mobile phones, but laptops can reach up to 100 meters with powerful transmitters (Hadlington, 2021).

Bluejacking allows phone users to send business cards anonymously using Bluetooth wireless technology. Bluejacking does not involve the removal or alteration of any data from the device. Bluejackers often look for the receiving phone to ping or the user to react. In order to carry out a bluejacking, the sending and receiving devices must be within 10 meters of one another. Phone owners who receive bluejack messages should refuse to add the contacts to their address book. Devices that are set in non-discoverable mode are not susceptible to bluejacking (Adam, 2021).

Bluejacking makes use of the Bluetooth technology to send unsolicited/unwelcomed messages to Bluetooth enabled devices. Receiver does not get to know who has sent the message to it. It only receives the message along with name and model of the sender’s phone. This technology is known as Bluejacking. Bluejacking is instigated by an attacker (termed as bluejacker or bluejack addict) who forwards unsolicited messages to a user of Bluetooth-enabled device. When the connection goes through, the bluejacker tries to send a message to the recipient. The actual message sent to the user’s device does not cause detriment, but is used to inveigle the user to counter react in some manner or add the new contact to the device’s address book (Diaz, Alejandra, & Anupam, 2020).

## BLUEJACKING TECHOLOGY

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e. for bluedating or bluechat) to another Bluetooth enabled device via the OBEX protocol (Rana, 2020).

This bluejack phenomenon started after a Malaysian IT consultant named “Ajack” posted a comment on a mobile phone forum. Ajack told IT Web that he used his Ericsson cellphone in a bank to send a message to someone with a Nokia 7650.

Becoming bored while standing in a bank queue, Ajack did a Bluetooth discovery to see if there was another Bluetooth device around. Discovering a Nokia 7650 in the vicinity, he created a new contact and filled in the first name with ‘Buy Ericsson!' and sent a business card to the Nokia phone (Kiren & Sunil, 2020).

**BLUETOOTH BLUEJACK**

[Bluetooth](https://electronics.howstuffworks.com/bluetooth.htm) technology operates by using low-power [radio](https://electronics.howstuffworks.com/radio.htm) waves, communicating on a frequency of 2.45 gigahertz. This special frequency is also known as the ISM band, an open, unlicensed band set aside for industrial, scientific and medical devices. When a number of Bluetooth devices are switched on in the same area, they all share the same ISM band and can locate and communicate with each other, much like a pair of [walkie talkies](https://electronics.howstuffworks.com/question530.htm) tuned to the same frequency are able to link up. Bluetooth technology users take advantage of this ability to network with other [phones](https://electronics.howstuffworks.com/cell-phone.htm) and can send text messages or electronic business cards to each other. To send information to another party, the user creates a personal contact name in his or her phone's address book, the name can be anything from the sender's actual name to a clever nickname (Adam, 2020).

Bluejackers have devised a simple technique to surprise their victims: Instead of creating a legitimate name in the address book, the bluejacker's message takes the place of the name. The prank essentially erases the "from" part of the equation, allowing a user to send any sort of comment he wishes without identifying himself. For instance, if you're sitting in a coffee shop and notice a fellow Bluetooth user sitting down to enjoy a cup of iced [coffee,](https://science.howstuffworks.com/innovation/edible-innovations/coffee.htm) you could set up a contact under the name "Is your coffee cold enough?" After choosing to send the text via Bluetooth, the phone will search for other enabled Bluetooth devices; selecting one will send the unsolicited message to that device. A bluejacker's crowning moment comes, of course, when the victim receives the message and expresses a mild mix of confusion and fear that he's under surveillance (Naaz, 2021).

Bluejacking is imprecise, however. Searching for other Bluetooth-enabled hardware might turn up a list of devices labeled with a series of numbers and letters. Unless the bluejacker’s target has chosen to publicly identify his or her phone, or it's the only Bluetooth phone in the area, the bluejacker may have a hard time messaging his or her target on the first try (Kiren & Sunil, 2020).

**HOW TO PREVENT BLUEJACKING**

Bluejacking is mostly used by people as a way to market their products and services. However, this is not an advisable and efficient way as it confuses the receiver, making him think that his device is malfunctioning. Although harmless, bluejacking can get annoying at times, as the recipient doesn’t know who the message sender is. Biswal and Kumar (2021), outlined certain ways by which it can be prevented on our devices, few of which have been mentioned below:

**Setting the Bluetooth on the Right Mode**

If you happen to use the Bluetooth connection more often, putting it off/on can be a chore. Adjust the setting of Bluetooth to non-discoverable mode. The non-discoverable mode hides the device from attackers or unknown people.

**Factory Reset of the Phone**

If your device was perpetrated at some point, it means that the attacker’s device has already been added as a trusted device on your phone. Reset the phone to take off all the devices from the trusted list.

**Keep Away from Strangers**

Make it a point to decline any messages or connection requests from unknown devices. Most attacks happen due to accepting connection requests from strangers who then get added as trusted devices.

**Keep the Device Updated and Password Character Strong**

Make sure you maintain strong passwords and change them at regular intervals. Keep your devices up-to-date with the latest technology.

**Putting off the Bluetooth When Not in Use**

If you don’t use the Bluetooth connection frequently, keep it off to avoid your device from being listed in the sender’s device search list. This method keeps the device safe from perpetrators who try to gain access to others’ phones using Bluetooth.

**Set Password for Bluetooth**

It is very simple to secure your device by setting a pin or a password for your Bluetooth connection. This will prompt a password from anyone trying to pair with your device. Remember to keep this password secure by sharing it only with trusted people.

One advantage of using latest technology gadgets like as iPhone or iPad is that bluejacking is restricted on them. Perpetrators, besides sending unsolicited messages, can also hack into confidential data from a victim’s device, thus, rendering him helpless. This is a much harmful form of hijacking, which is called [bluesnarfing.](https://techspirited.com/what-is-bluesnarfing-how-to-prevent-it)

Almost everyone today has a smartphone and one of the features that comes standard is Bluetooth capability. Since your device has Bluetooth capabilities, it also has the capability to be hacked. If your smartphone is hacked via Bluetooth connection, you are potentially at risk of losing your phone’s data, pictures, videos, messages, contacts, and other information compromised. Today if you own a smartphone, you are walking around with a small computer in your pocket (Jampen, 2020).

**Applications of Bluejacking**

#### 1. Viral communication

Exploiting communication between consumers to share content such as text, images and Internet references in the same way that brands such as Budweiser, Honda, Trojan Condoms and even John West Salmon, have created multimedia content that has very quickly been circulated around the Internet

#### 2. Community activities

Dating or gaming events could be facilitated using Bluetooth as a channel to communicate between participants. The anonymous nature of bluejacking makes is a superb physiological tool for communication between individuals in a localized environment such as a café or pub.

**3. Location based services**

Bluejacking could be used to send electronic coupons or promotional messages to consumers as they pass a high street shop or supermarket. To date SMS text messaging has been used with mixed success as a mechanism to send consumer’s location based information Rainier PR believes that viral communication and to a lesser extent event based activities offer the greatest opportunity for bluejacking as a marketing mechanism.

### Advantages of Bluejacking

1. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well
2. People can send any image or sound but not insulting.
3. Any copyright sound files will only be sent with the written consent of the copyright holder.
4. We can easily transfer data from mobile to laptop or from mobile to mobile in a short period.
5. We can even enjoy music by wireless headphones through Bluejacking.

### Disadvantages of Bluejacking

1. But with the increase in the availability of Bluetooth enabled devices, these devices have become vulnerable to virus attacks and even complete takeover of devices through a Trojan horse program. These may even cause irritation in any person as these are just unwelcomed messages or some jokes.
2. They can annoy anyone very easily.

## FUTURE ASPECTS OF BLUEJACKING

Looking at its current use and misuse also by few people, it is expected that in the future, it may have the following aspects. Either it will be used extensively and people would be able to get all the necessary information on their devices if they have their Bluetooth on, Or people will stop using Bluetooth even and only bluejackers will be playing with each other, Or some new way could be developed in order to find the location of the device sending a blue jack request and their location can be traced. If they keep send annoying messages, we can find them out and can register a complaint against them. By this way, Bluetooth will be made more reliable (Naaz, 2021).

## CONCLUSION

In conclusion, it can be said that bluejacking is not at all harmful. By it, we can interact with new people. The only thing it can do at worst is to irritate you or annoy you by sending unsolicited messages but you can still prevent yourselves from these messages by changing the visibility of your Bluetooth to invisible or non-discoverable mode.

**RECOMMENDATIONS**

It can be helpful as well by providing you with lots of useful information as well.

1. So, this seminar paper recommends that this technology be used properly as it is intended and get best of it, rather than just making wrong use of it and irritating others.
2. It is also recommended that best practices to mitigate the Bluejacking threats against the Bluetooth are: user awareness, disable device when not in use, use an unidentifiable device name, employ security mode 3 or 4, disable unused services and profiles, set device to non-discoverable mode when not in use, use non-guessable PIN codes of at least 12 or more alphanumeric characters and perform pairing only when absolutely required.

# **REFERENCES**

Adam, K. (2021). *Bluejacking*. McGraw Hill, New York.

Biswal, C. & Kumar, P. (2021). Cyber‐Crime Prevention Methodology. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications* (2021): 291-312.

Diaz, A., Alejandra, T. & Anupam, J. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), 53-67.

Hadlington, L. (2021). The “human factor” in cybersecurity: Exploring the accidental insider. *Research Journal of Artificial Intelligence Applications in Security, 2(32),* 45-75

Jampen, D. (2020). Mining Bluetooth Attacks in Smart Phones. A comparative literature reviews. *Journal of Human-centric Computing and Information Sciences,* 10(2), 1-41.

Kiren, D. & Sunil, N. (2020). "Different Types of Bluetooth Attacks and Detection Techniques: A Review." *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*. IEEE.

Naaz, S. (2021). Understanding Bluetooth Range." *International Journal of Digital Crime and Forensics (IJDCF)*, 13(2), 1-15.

Rana, A. (2020). Bluejacking processes and attacks survey: Types, vectors, and technical approaches. *Journal of Digital Communications and Networks,* 6(2), 147-156.