

**BLDE Association's  
S B Arts and K C P Science College, Vijayapur**

**Department of M.Sc. Computer Science**

**Date: 12/03/2018**

**NOTICE**

**This is informing to all the M.Sc. CS-II and IV Semester students to attained TED TALK on 13-03-2018 at 12:15pm in L.H. NO -01 Topic: "How hacking can be done?"**

**Co-ordinator**

M.Sc. (C.S.) Programme  
S.B.Arts & K.C.P.Science College,  
Vijayapur.



**IQAC, Co-ordinator**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.



**Principal**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.



**B.L.D.E. Association's**

**S.B.ARTS & K.C.P SCIENCE COLLEGE  
VIJAYAPUR**

**A REPORT ON**

**TED Talk**

**on**

**“How Hacking can be done?”**

**On**

**13<sup>th</sup> March 2018**

**For**

**For I and III Sem M.Sc (CS) Students**

**Conducted by**

**Prof. Smt R D Joshi**

**AY**

**2017-18**

## A Report on a Ted-Talk

**Presenter** : Prof. Rajashree D Joshi M.Sc (C.S)

**Title** : How Hacking can be done?

**Date given** : March 13, 2018

**Link** : <https://youtu.be/hqKaf17Am88>

---

### **Hacking**

In some cases, hackers steal credit card numbers by hacking businesses. Many web commerce systems allow you to store your credit card information for later use, making repeated purchases easy. Most businesses heavily encrypt this information, so that even if a hacker manages to steal the database, decoding the individual credit card numbers is impossible. Unfortunately, occasional security flaws allow criminals to bypass this security, allowing them to steal large numbers of cards at once. If your credit card supports the technology, single-use card numbers can prevent hackers from accessing your accounts even if they compromise card databases. At the very least, you should resist the urge to allow sites to store your credit card details between sessions.

### **Skimming**

The Internet is not the only way a criminal can steal your credit card number. Skimmers are electronic devices, usually placed on ATMs or the card readers on gas pumps. When you place your card into the reader, it passes through the skimmer, allowing the device to capture your account information. Travelers are especially vulnerable to these devices, since they may be unfamiliar with the normal pump or ATM design. Always examine outdoor card readers carefully before using them, and look for anything that seems out of place or awkwardly attached.

### **How Do Hackers Get Your Card Number?**

Opening up your credit card statement and seeing charges you did not make is never a pleasant experience. All too often, hackers target businesses with the ultimate goal of stealing financial information like credit card numbers, trophies they trade to other cyber criminals or simply use to run

up bogus charges. Hackers steal credit card numbers in a variety of ways, and understanding these methods can help your company avoid becoming a victim.

There are different types of hacking:

1. **Phishing:** One of the simplest and most direct methods of card theft is phishing. The hacker simply calls your business, pretending to be from your bank, and tricks you into giving away your financial data. Often, phishing attempts begin with a warning of unauthorized activity to put you on your guard and make you eager to cooperate. If you ever receive a call claiming to be from your bank or card issuer, do not provide any account information and call your bank directly to report the contact.

2. **Spoofing:** Hackers can also use fake emails and websites to steal credit card information. Much like a phone phishing attack, a spoofed email will claim to be from your financial institution and report some kind of fraudulent access to your business account. The email will claim that all you need to do to correct the problem is log into their site with the link provided and enter your account information to verify your identity. Of course, the link goes to a fake site the hacker controls, designed to capture any data you enter. If you receive an email claiming to be from your card issuer, do not click any links, and call your provider for further information.

### **How to Deal With Stealing In the Workplace**

Although money is the first thing that comes to mind, stealing in the workplace isn't necessarily limited to cash. Employees can steal proprietary company information and pass on confidential information to your competitors. On a smaller scale, employees can steal supplies, property and even time from the business by conducting personal matters on company time. In a small business, stealing by a single employee can have a significant negative impact on both productivity and the bottom line. A thieving employee won't advertise his illegal activities, so managers must be alert to any suspicious signs and be prepared to investigate when necessary.

1. **Identify the missing money or supplies.** Review company accounts, bills and statements to reveal inconsistencies. Explore other explanations and potential reasons for the discrepancy -- don't automatically jump to the conclusion that an employee is stealing.

up bogus charges. Hackers steal credit card numbers in a variety of ways, and understanding these methods can help your company avoid becoming a victim.

There are different types of hacking:

1. **Phishing:** One of the simplest and most direct methods of card theft is phishing. The hacker simply calls your business, pretending to be from your bank, and tricks you into giving away your financial data. Often, phishing attempts begin with a warning of unauthorized activity to put you on your guard and make you eager to cooperate. If you ever receive a call claiming to be from your bank or card issuer, do not provide any account information and call your bank directly to report the contact.

2. **Spoofing:** Hackers can also use fake emails and websites to steal credit card information. Much like a phone phishing attack, a spoofed email will claim to be from your financial institution and report some kind of fraudulent access to your business account. The email will claim that all you need to do to correct the problem is log into their site with the link provided and enter your account information to verify your identity. Of course, the link goes to a fake site the hacker controls, designed to capture any data you enter. If you receive an email claiming to be from your card issuer, do not click any links, and call your provider for further information.

### **How to Deal With Stealing In the Workplace**

Although money is the first thing that comes to mind, stealing in the workplace isn't necessarily limited to cash. Employees can steal proprietary company information and pass on confidential information to your competitors. On a smaller scale, employees can steal supplies, property and even time from the business by conducting personal matters on company time. In a small business, stealing by a single employee can have a significant negative impact on both productivity and the bottom line. A thieving employee won't advertise his illegal activities, so managers must be alert to any suspicious signs and be prepared to investigate when necessary.

1. **Identify the missing money or supplies.** Review company accounts, bills and statements to reveal inconsistencies. Explore other explanations and potential reasons for the discrepancy -- don't automatically jump to the conclusion that an employee is stealing.

**2. Watch for red flags if you can't immediately identify which employee is stealing.** According to the U.S. Small Business Administration, behaviors to look out for include a preference for taking work home or working after hours without supervision, a reluctance to take time off or let others assist with job responsibilities -- so that the stealing cannot be discovered -- and unanticipated changes in the employee's behavior.

**3. Investigate the issue.** Interview the suspected employee and others who may have witnessed the activity. Review documents -- bank statements, emails and check registers, for example -- and use other relevant information such as access card records, time clock data and footage from security cameras to confirm your suspicions. Remain neutral and objective while you collect the facts.

**4. Discipline the employee.** Consider all the mitigating circumstances, the severity of the theft, whether the theft was intentional and the amount of dishonesty involved when deciding the level of discipline to impose. In most cases, the company will likely decide to fire the stealing employee.

**5. Recover the loss by referring the theft for prosecution, suing the employee, recovering through insurance or a combination of these approaches.** Consider less costly alternatives to litigation -- such as a repayment agreement with the employee -- depending on the severity of the issue and the employee's willingness to cooperate. Weigh the pros and cons of legal action. For example, requiring your employees to testify in court about the theft impacts productivity on those days, but also sends a strong message to staff that the company does not tolerate employee theft and will prosecute stealing to the fullest extent of the law.

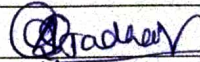

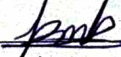
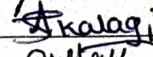
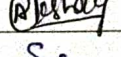


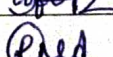
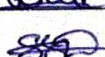
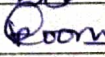
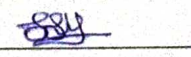

**6. Implement preventative measures for the future.** Identify causes for theft and increase operational controls to prevent the issue. Review policy and procedure to identify any weaknesses and enforce a zero tolerance approach to employee theft and dishonesty. Consider cross training employees and rotating their duties so that no single employee is responsible for an operational area.

**B.L.D.E.A's**  
**S B Arts and K C P Science College, Vijayapur**  
**M.Sc(CS)**

**TED TALK TITLE:HOW HACKING CAN BE DONE?**

Date:13/03/2018

TIME: 2:00 PM


SL.NO	STUDENT NAME	SEMESTER	SIGNATURE
1	Ambika. S. Jadhav	II	
2	Saumya. V. Hiremath	II	
3	Pooja. M. Bixadar	II	
4	Akshata. S. Kalagi	II	
5	Akshay Kumar. A. Patil	II	
6	Sounhya. Narasana Gowda	IV	
7	Vijayalaxmi. Bantwal	IV	
8	Roope Dhaswad	IV	
9	Rukha Rathod	IV	
10	Shrigaori. S. Doragi	IV	
11	Poojima. B. Hauji	IV	
12	Shobha. S. Yalage	IV	
13			
14			
15			
16			

Staff : 

**IQAC, Co-ordinator**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

  
Co-ordinator:  
**Co-ordinator**

BCA Programme  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

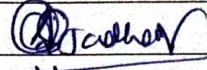

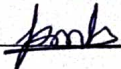
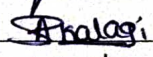
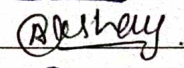
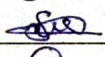

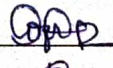
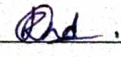
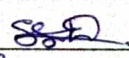
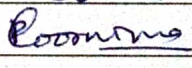
  
**Principal**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

**B.L.D.E.A's**  
**S B Arts and K C P Science College, Vijayapur**  
**M.Sc(CS)**

**TED TALK TITLE:HOW HACKING CAN BE DONE?**

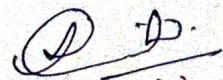
Date:13/03/2018

TIME: 2:00 PM

SL.NO	STUDENT NAME	SEMESTER	SIGNATURE
1	Ambika. S. Jadhav	II	
2	Soumya. V. Hiremath	II	
3	Pooja. M. Birsadar	II	
4	Akshata. S. Kalagi	II	
5	Akshay Kumar. A. Patil	II	
6	Soumya Khasanagoudra	IV	
7	Vijayalaxmi. Bantanal	IV	
8	Roopre. Dhaswad	IV	
9	Rekha Lathod	IV	
10	Shriparvati. S. Doraji	IV	
11	Poornima. B. Hanji	IV	
12			
13			
14			
15			
16			

Staff: 

**IQAC, Co-ordinator**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

  
Co-ordinator:

**Co-ordinator**  
BCA Programme  
S.B.Arts & K.C.P.Science College,  
Vijayapur.

  
**Principal**  
S.B.Arts & K.C.P.Science College,  
Vijayapur.