CYBER SECURITY TIPS

(Email, mobile, credit/debit card, etc)

Computer Centre
Manipur University
Contents

1 Objective ............................................. 1
2 Introduction ......................................... 1
3 Safety tips for using Email ......................... 1
4 Secure Usage of Credit & Debit Card/ATM ............ 1
5 Mobile Phone Security ............................... 2
   5.1 Do’s .............................................. 2
   5.2 Don’ts ............................................. 3
6 Staying Safe on Social Networking Sites ............. 3
7 Conclusion ........................................... 3

List of Tables

List of Figures
1 Objective
The principal objective of this literature is to help end users (technical as well as non-technical computer users) become more cyber aware and inform them on how to stay alert and be safe online.

2 Introduction
Most of the biggest cybersecurity incidents occur because of human error. This can include mistakes like leaving accounts open on shared computers, failing to update passwords regularly, accidentally downloading malicious files, and giving away information through phishing scams.

Educating end users about proper cyber security can mitigate some of the risks. User awareness is the strongest defence against data breaches, account hacking, phishing, etc.

3 Safety tips for using Email
Source: CERT-IN
To minimize the risk of information leakage and account hacking, there are some recommendations to be followed by an user for using email in a secure way. These recommendations are as follows.

i Be suspicious while opening unexpected emails. Do not open suspicious email Attachments.
   Do not open untrusted/unknown emails (spam)

ii Avoid clicking of unknown/untrusted web-links provided in email messages to prevent secretly installation of a malware (e.g., virus) on your computer

iii Do not respond suspicious/banking-related (Phishing)/winning lottery/fund transfer emails to avoid becoming a victim of financial frauds.

iv Install latest Anti-virus/Anti-Spyware software and keep them up-to-date. Keep Operating System and application software updated with latest security updates / patches in the computer system used for email to prevent the exploitation of the weakness in the system.

v Avoid exposure of E-Mail account details such as user name and password to unknown/unauthorized persons while using E-Mail.

vi Keep strong password with minimum of eight characters, comprising a combination of alphabets (both upper and lowercase), numbers and special characters.

vii Scan an email attachment before opening/downloading to minimize the risk of downloading malware (e.g., virus).

viii Enable spam filter to reduce amount of spam/junk emails

ix Do not keep your computer unattended to avoid misuse

4 Secure Usage of Credit & Debit Card/ATM
Source: CERT-IN

i Don’t accept the card received directly from bank in case if it is damaged or seal is open.

ii Don’t write your PIN number on your credit card.

iii Don’t disclose your Credit card number/ATM PIN to anyone.

iv Don’t hand over the card to anyone, even if he/she claims to represent the Bank.
v Don’t get carried away by strangers who try to help you use the ATM machine.

vi Don’t transfer or share your account details with unknown/non validated source.

vii Don’t access Netbanking or make payments using your Credit/Debit card from shared or unprotected computers in public places.

viii Don’t give out your account number over the phone unless you initiate the call and you know the company is reputable.

ix Don’t provide credit card information on a website that is not a secure site. Some signs of a secure site are a lock image at the bottom of your browser and a URL that begins with https.

x Don’t share any confidential information such as password, customer id, Debit card number, Pin CVV2, DoB to any mail requests, even if the request is from government authorities like Income Tax department, RBI or any card association company like VISA or Master card.

xi Don’t address or refer to your bank account problems or your account details and password on social networking sites or blogs.

xii Don’t store critical information like your ATM PIN number in your mobile phone.

5 Mobile Phone Security

Source: CERT-IN

Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. Mobile phones can be infected with worms, trojan horses or other virus families, which can compromise your security and privacy or even gain complete control over the device.

5.1 Do’s

i Record IMEI (International Mobile Equipment Identity) number. This is usually printed on the phone below the battery, or can be accessed by keying *#06# on most of the phones. In case Mobile phone is stolen/lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

ii Use autolock to automatically lock the phone or keypad lock protected by passcode/security patterns to restrict access to your mobile phone.

iii Use a PIN to lock SIM card: Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN.

iv Use the feature of Mobile Tracking which could help if the mobile phone is lost/stolen.

v Update the mobile operating system regularly and upgrade the operating system to its latest version.
vi Always install applications from trusted sources.

vii Consider installing security software from a reputable provider and update them regularly.

viii It’s always helpful to check the features before downloading an application. Some applications may use your personal data.

ix If you’re downloading an app from a third party, do a little research to make sure the app is reputable.

5.2 Don’ts

i Never leave your mobile device unattended.

ii Turn off applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections on may pose security issues and also cause to drain out the battery.

iii Never allow unknown devices to connect through Bluetooth.

iv Never switch on Bluetooth continuously.

v Never put Bluetooth in always discoverable mode.

vi Never connect to unknown networks or untrusted networks.

6 Staying Safe on Social Networking Sites

Source: https://www.us-cert.gov/ncas/tips/ST06-003

i Limit the amount of personal information you post such as your address or information about your schedule or routine.

ii Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can’t retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people’s machines.

iii Be wary of strangers.

iv Be skeptical - Don’t believe everything you read online. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.

v Be wary of third-party applications

vi Use strong passwords

vii Check privacy policies - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam.

viii Keep software, particularly your web browser, up to date.

7 Conclusion

Refer to Indian Computer Emergency Response Team, CERT-IN for more information on how to improve your cybersecurity posture and protect yourself from cyberattacks.