National Institute of Electronics and Information Technology, Imphal

Common Internet Threats:

As the World Wide Web has evolved over the years, many Internet nasties have been playing on vulnerabilities to attack computers and retrieve sensitive data from individuals. Half the time, we aren't even aware it is happening until it is too late.

There are many malicious threats you need to dodge along the way.

Botnets

- If you've never heard of a botnet, it's likely because they go largely undetected.
- A collection of software robots, or 'bots', that creates an army of infected computers (known as 'zombies').
- They are remotely controlled by the originator.
- Yours may be one of them and you may not even know it.

Hacking

- Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer.
- The process by which cyber criminals gain access your computer.

Malware

- Malware is one of the more common ways to infiltrate or damage your computer.
- Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware.

Pharming

- Pharming is a common type of online fraud.
- A means to point you to a malicious and illegitimate website by redirecting the legitimate URL.
- Even if the URL is entered correctly, it can still be redirected to a fake website.

Phishing

- Phishing is a form of **internet scam** whereby "phishers" target customers of banks and financial institutions, and try to trick them to divulge sensitive personal information (such as credit card details or PIN numbers).
- Phishers normally use spoof emails and fake websites that look authentic.

Ransomware

- Ransomware is a type of malware that restricts access to your computer or your files and displays a message that demands payment in order for the restriction to be removed.
- The two most common means of infection appear to be **phishing emails that contain malicious attachments** and **website pop-up advertisements**.

Spam

- Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people.
- The mass distribution of unsolicited messages, advertising or pornography to addresses.
- This message is any electronic message that encourages participation in a commercial activity, regardless of whether there is an expectation of profit.

Keyloggers

Similar to a part of spyware, keyloggers record a user's keyboard actions. Most keyloggers will be looking for distinguishable key entries, such as bank card details and passwords. Keylogging is often linked to identity and intellectual property theft.

Spyware

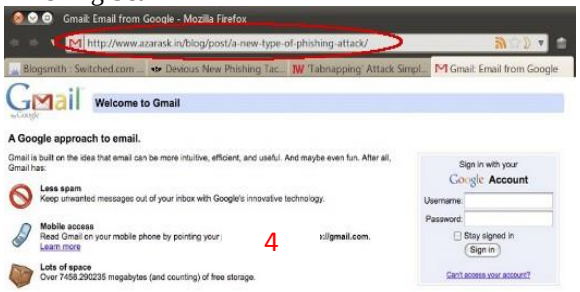
Another form of malware is spyware. Once installed on your computer, spyware can monitor your keystrokes, read and delete your files, reformat your hard drive, and access your applications. Whoever is controlling the spyware has access to your personal details without you even knowing.

Software Piracy:

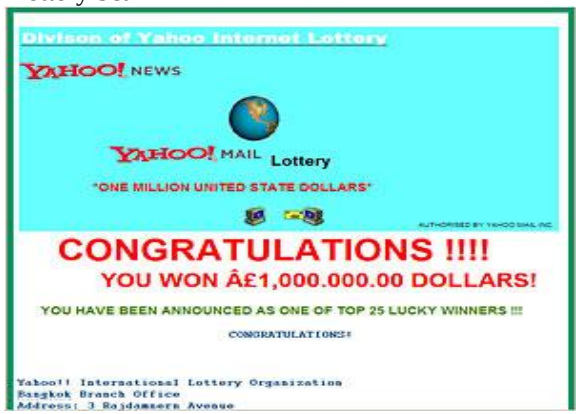
- Theft of software through the illegal copying of genuine programs.
- Distribution of products intended to pass for the original.

Some Common Scams:

- Phishing Scam



- Lottery Scam



- Online Auction
- Forwarding or Shipping
- E-mail Scam

Rules to make yours password strong

- At least 8 characters—the more characters, the better
- A mixture of both uppercase and lowercase letters
- A mixture of letters and numbers
- Inclusion of at least one special character, e.g., ! @ # ?]

  Note: do not use < or > in your password, as both can cause problems in Web browsers

Tips for keeping your password secure

- Change it regularly—once every three to six months.
- Change it if you have the slightest suspicion that the password has become known by a human or a machine.
- Never use it for other websites.
- Avoid typing it on computers that you do not trust; for example, in an Internet café.
- Never save it for a web form on a computer that you do not control or that is used by more than one person.
- Never tell it to anyone.
- Never write it down.

Consumers wanting to be as safe as possible when shopping online should take several key steps.

1. Passwords

   • Use a hard-to-guess password that contains upper and lower case letters, numbers and symbols.

   • Do not use the same user name and password for all online accounts.

   • Change passwords as often as possible, but at least every three months.

2. Online shopping tips

   • Always log out of bank, credit card, and merchant sites after you have completed your transaction.

   • Do not allow your computer to store user names and passwords for merchant or banking websites.

   • When setting up security questions for sites online, use false information unrelated to your personal information, and keep track of your answers.

3. Secure E-Commerce websites

   • Use a reputable third-party pay service for online transactions whenever possible. These sites provide secure transactions and dispute resolution services.

   • Secure online transactions should occur only on a website that begins with "https://." Do not trust a vendor without the "S" after "http" at the start of the web address.

4. Where not to shop

   • Do not shop, pay bills, or access your bank or credit card websites using public Wi-Fi. Shop from home and only over a secured Internet connection.

   • Do not use "easy pay" payment options or "one-click ordering." It takes a few extra seconds to enter a user name and password on a merchant site but often takes months to recover from online credit card fraud.

5. How to shop safely

   • Pay attention when visiting financial and sales websites. Authentic websites will post logos such as that for VeriSign.

   • Use only one credit card for online purchases in order to limit exposure to fraud and theft on all your cards. If possible, use a pre-paid debit card in place of a credit card.

6. Keep impeccable records

   • Keep records of every Internet purchase and transaction, and compare them with credit card and bank statements monthly. Report any

discrepancies immediately to the issuer of the card.

7. Firewalls

• Always use the most up-to-date version of a strong anti-virus and firewall security program.

• Download and apply updates from your virus and firewall programs when available, to ensure your program has the latest information about new scams and hacker tricks.

8. Anti-Virus Programs

• Run virus scans regularly on your computer.

• Use an ad-blocking software program and a spyware detection program. Keep these programs updated and run scans often with them.

9. Personal information protection

• Do not post your full birth date on social networking sites such as Facebook. Do not post the birthdates of your children, spouse, or significant other.

• Any information you post online can be hacked and stolen, so try to keep this information to a minimum.

10. Email security

• If an email, instant message, chat request or Internet site appears suspicious, close your browser and email programs and shut down your computer for a time. When you restart the computer, run a full virus and spyware scan before logging back on to the Internet.

Worst case scenario

• If you ever suspect your credit card or personal information has been used online without your permission, immediately contact the major credit reporting agencies to place a fraud alert on your credit report.

Tips to use internet banking safely:

1. Always use genuine anti-virus software
2. Avoid Using Public Wi-Fi or Use VPN software
3. Check for latest updates of your Smartphone's operating system
4. Change your password regularly and ensure it's a strong one
5. Subscribe for mobile notifications
6. Avoid signing-in to your net-banking account via mailers
7. Do not use public computers to login to net banking
8. Check your account regularly

How will you know if your computer is infected?

Here are a few things to check for:

- It takes longer than usual for your computer to start up, it restarts on its own or doesn't start up at all.
- It takes a long time to launch a program.
- Files and data have disappeared.
- Your system and programs crash constantly.
- The homepage you set on your web browser is different (note that this could be caused by Adware that has been installed on your computer).
- Web pages are slow to load.
- Your computer screen looks distorted.
- Programs are running without your control.