Contemporary Issues – Report Submissson

THE RISING ERA OF CYBER SECURITY IN INDIA

REPORT SUBMISSION

Assignment Submitted to:

Dr. Vivek Srivastava (Associate Professor)

NIIT University, Neemrana

By Siddharth Swain (M.Tech GIS, 2nd Year)

NIIT University, Neemrana

TABLE OF CONTENTS

1. INTRODUCTION

Security is becoming a rapidly evolving and complex issue that various organizations are contending with today. It continues to be one of the most pressing challenges faced by Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) today. With the increasing impact of social media, smart devices and mobility, organizations are becoming more vulnerable to fraud and privacy breaches. Globally, security has risen to be one of the top concerns in almost all areas from defence, corporate organization, smart cities, etc.

With the increasing volume of data generated by organizations, instances of cyber-attacks, loss of sensitive information, and security breaches are becoming increasingly common. Increasing internet penetration is leading to expansion of cyber space which in turn is leading to increasing attacks on sensitive intellectual property. This has resulted in the transformation of the IT landscape at a very rapid pace.

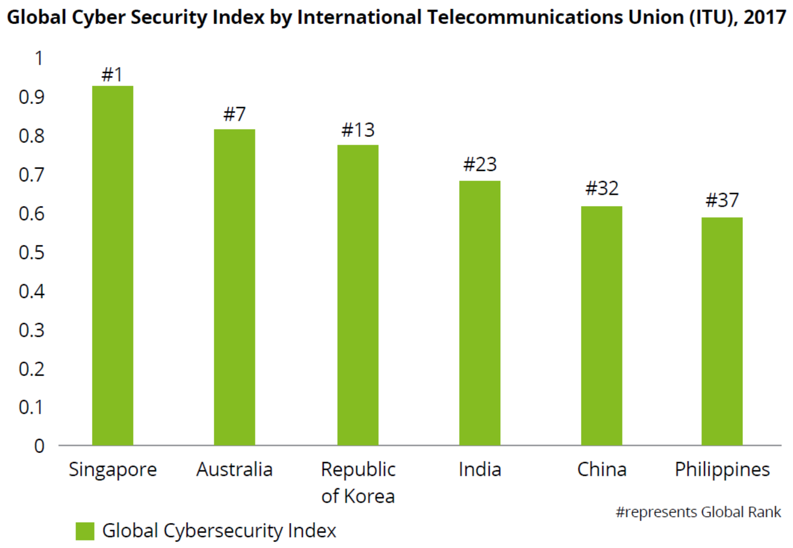


Fig. 1 Global Cybersecurity Index (The # represents the Country's Global Rank)

According to The Global Cyber Security Index released by the UN telecommunications agency International Global Cyber Security Index by International Telecommunications Union (ITU), 2017 Telecommunication Union (ITU) in 2017, only about half of all countries have a cybersecurity strategy or are in the process of developing one. The index, which saw India at 23rd position, was topped by Singapore at 0.925. India has also been ranked fourth globally among the countries most affected by ransomware.

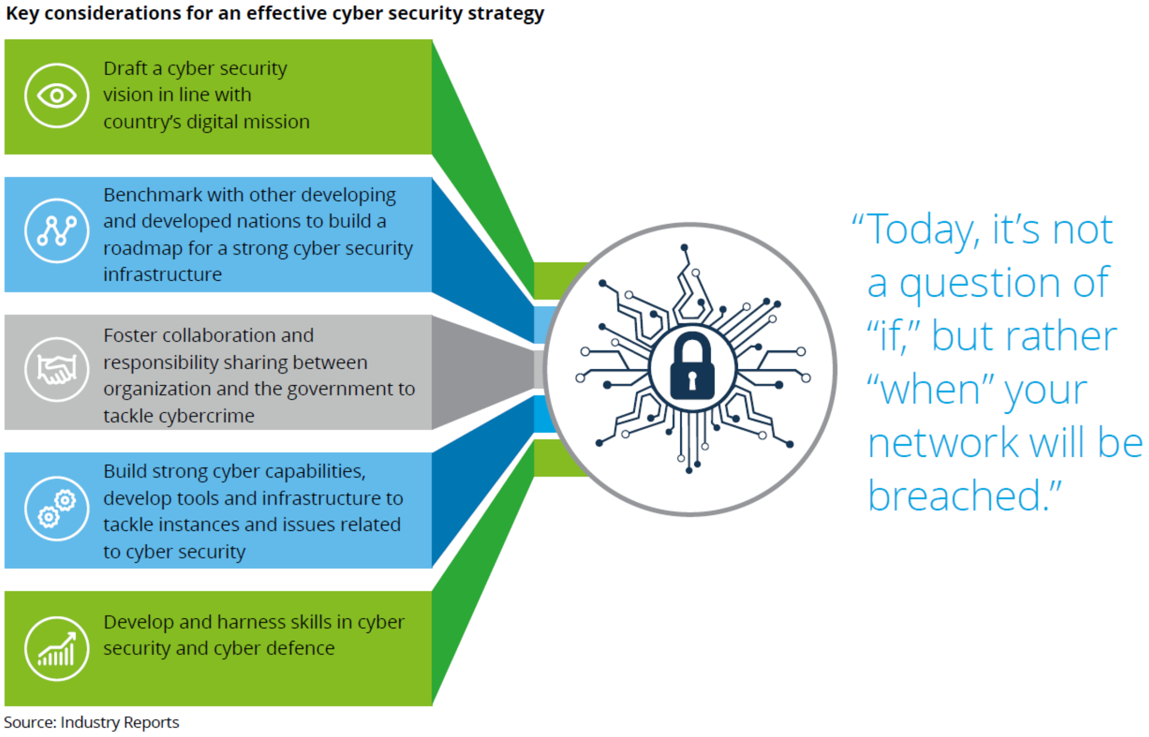

Key considerations for an effective cyber security strategy
Draft a cyber security vision in line with country's digital mission
Benchmark with other developing and developed nations to build a roadmap for a strong cyber security infrastructure
Foster collaboration and responsibility sharing between organization and the government to tackle cybercrime
Build strong cyber capabilities, develop tools and infrastructure to tackle instances and issues related to cyber security
Develop and harness skills in cyber security and cyber defence
"Today, it's not a question of "if," but rather "when" your network will be breached."
Source: Industry Reports

Fig. 2 Key Considerations for an effective Cyber Security Strategy

1.1 Trends Resulting in Increased Focus on Cyber Security

Security is becoming a growing concern for organizations across domains due to increasing instances of cyber-attacks and changing technology landscape, consumer behaviour and regulatory requirements. Some trends which lead to increased focus on cyber security are listed below:

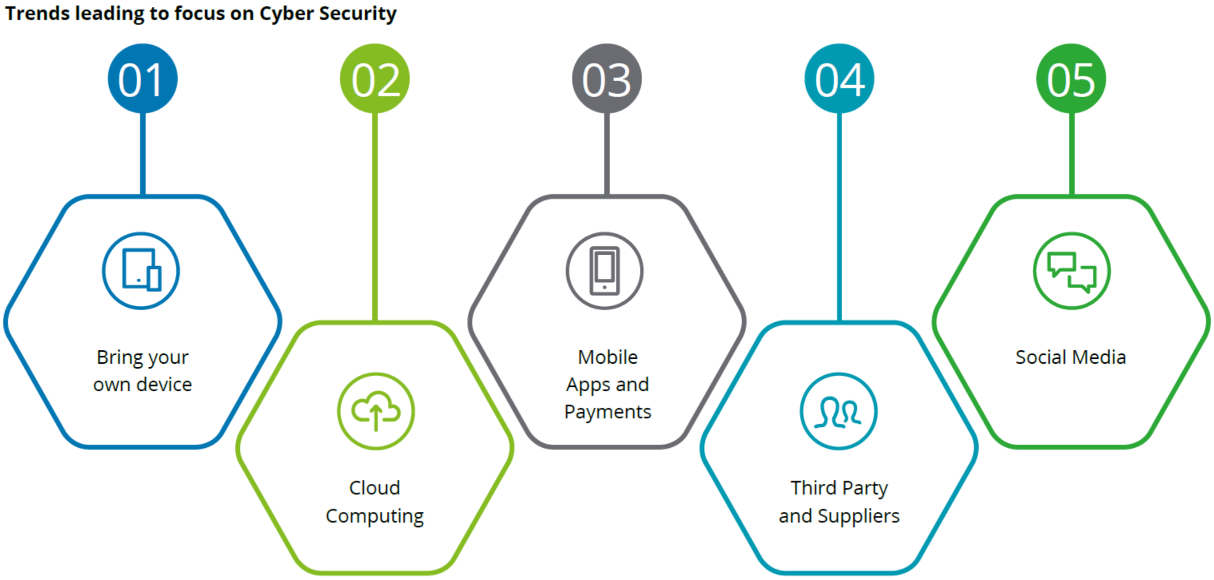


Fig. 3 Trends leading to the focus on Cyber Security

1.2 Bring You Own Device (BYOD)

Today, employees own powerful devices (smartphones, tablets) in order to fulfil their requirement of working anytime and anywhere and handle most of the business activities related to emails, documents, spreadsheets, etc. These devices are also used for extensive use of social media and accessing data stored on cloud. Use of business data and personal applications on a single device makes the device an easy target for attackers. There is an increased risk due to these devices since a large number of them are not managed by the organization's IT department.

1.3 Cloud Computing

Many organizations make use of cloud computing for their applications and data. This may lead to ease of use but often trumps security if it is not managed well. Since it is difficult to determine the physical location of the data stored in the cloud we might not know which regulations apply to it. Applications and data managed from outside the organization through cloud increases the organization's vulnerability to security risks.

1.4 Third Parties and Suppliers

Today, in this world of outsourcing, digital supply chains and cloud computing, organizations are more dependent than ever on third parties. This results in organization's data being shared and exposed in ways which are difficult to control. A breach in the digital supply chain undermines the security of every organization involved in the chain.

1.5 Mobile Apps and Payments

In order to grow the business, various organizations (like e-Commerce players etc.) are launching mobile applications for their users. They encourage users to make mobile payments. Authorities are promoting payment through mobile/digital means instead of cash. Though this is a valuable proposition for all stakeholders, inclusion of monetary transactions could increase the cyber risk exposure.

1.6 Social Media

Use of social media has increased drastically over the last few years. Increasing internet infrastructure and data availability, decreasing data charges and advent of cheaper smartphones have enabled the users to access social media and share information more frequently. Such increase in sharing of information has resulted in revealing sensitive information posing privacy-related issues.

1.7 Cyber Security Capabilities

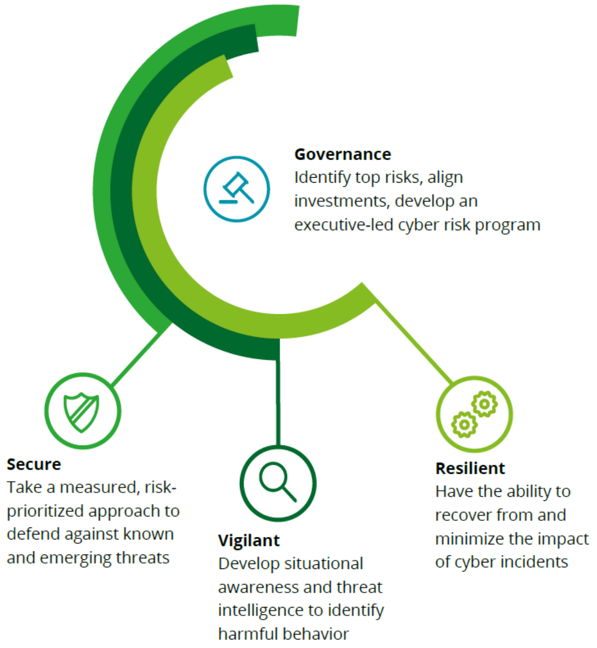

Governance
Identify top risks, align investments, develop an executive-led cyber risk program
Secure
Take a measured, risk-prioritized approach to defend against known and emerging threats
Vigilant
Develop situational awareness and threat intelligence to identify harmful behavior
Resilient
Have the ability to recover from and minimize the impact of cyber incidents

Fig. 4 Major Capabilities of Cyber Security

Other capabilities include:

Information Assurance

- Vulnerability Assessment
- Penetration Testing
- Information Security Assessment
- Application Security Evaluation
- Network Traffic Assessment
- Critically Assessment

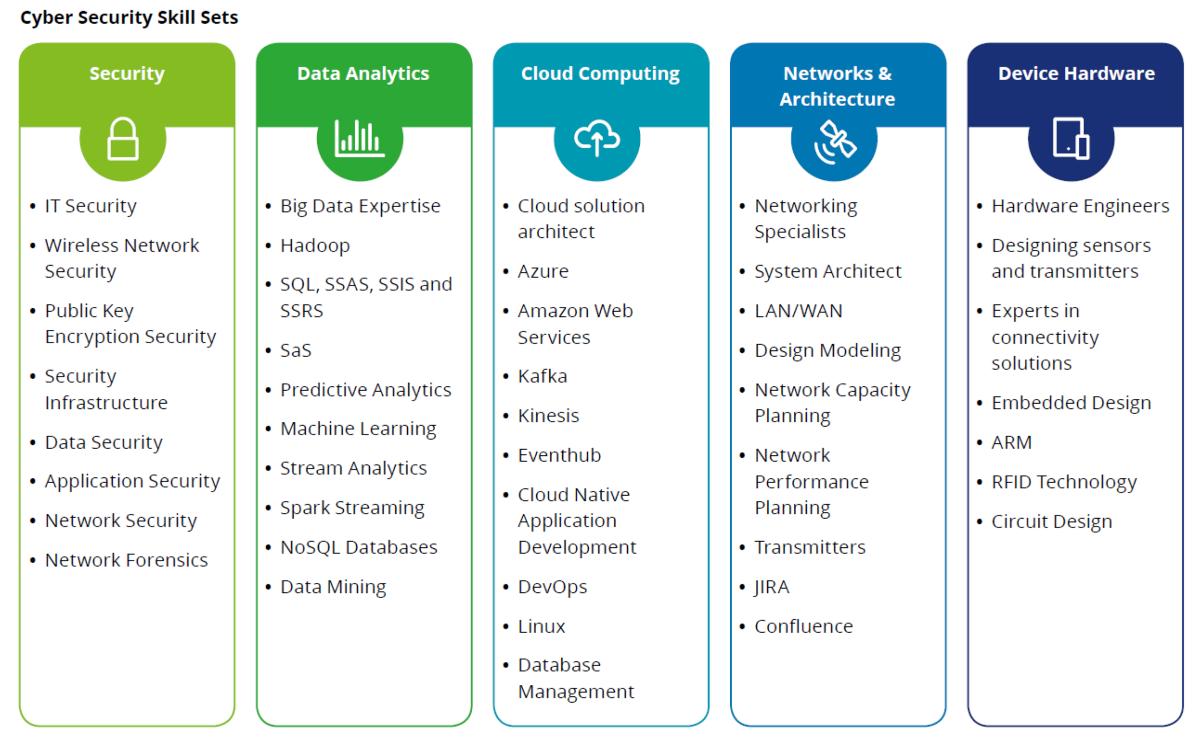
Risk/Vulnerability and Assessment Mitigation

- Threat, vulnerability and risk assessments
- Continuous vulnerability identification and assessment
- Threat intelligence
- Incident Response

Network Security

- Security Operations
- Managed Security Services
- Information Security

1.8 Cyber Security Skill Sets



Cyber Security Skill Sets

Security

- IT Security
- Wireless Network Security
- Public Key Encryption Security
- Security Infrastructure
- Data Security
- Application Security
- Network Security
- Network Forensics

Data Analytics

- Big Data Expertise
- Hadoop
- SQL, SSAS, SSIS and SSRS
- SaS
- Predictive Analytics
- Machine Learning
- Stream Analytics
- Spark Streaming
- NoSQL Databases
- Data Mining

Cloud Computing

- Cloud solution architect
- Azure
- Amazon Web Services
- Kafka
- Kinesis
- Eventhub
- Cloud Native Application Development
- DevOps
- Linux
- Database Management

Networks & Architecture

- Networking Specialists
- System Architect
- LAN/WAN
- Design Modeling
- Network Capacity Planning
- Network Performance Planning
- Transmitters
- JIRA
- Confluence

Device Hardware

- Hardware Engineers
- Designing sensors and transmitters
- Experts in connectivity solutions
- Embedded Design
- ARM
- RFID Technology
- Circuit Design

Fig. 5 Cyber Security Skill Sets

India is facing a huge scarcity of Cyber Security professionals especially at the leadership level which has increased salaries for such roles over 25-35 percent over the past year. Hacking and cyberattacks are compelling firms to hire talent at a premium, with compensation packages for top roles at upwards of Rs 2 crore, and in some instances, close to Rs 4 crore, inclusive of variables. In addition, last year's demonetisation and the government's push for Digital India (NSE 0.00 %) have pushed demand for cybersecurity talent. "Companies are now vulnerable to cyberattacks and especially with the government's initiatives like Digital India and demonetisation, almost all companies across all sectors are going digital to some extent," said Ashok Pamidi, senior director of Nasscom.

Financial services institutions including banks, payment gateways and ecommerce organisations are the biggest employers in cybersecurity, according to Sunil Goel, managing director at GlobalHunt.

The job profiles in cybersecurity include information risk auditors, firewall development professionals and security device development professionals, security analysts, intrusion detection specialists, computer security incident responders, cryptologists, vulnerability assessors, lead security architects, etc.

Though most organizations realize the importance of cyber security for their businesses and understand the associated risks, they often come short of a holistic, business-driven and threat-based approach to manage cyber risks. While securing assets is important, being vigilant and resilient in the face of cyber-attacks is imperative. Along with cybersecurity policies, tools, and practices, cultivating a cyber-risk aware culture across the organization will increase their ability to effectively manage emerging cyber risks.

2. THE ATTACK LANDSCAPE

The year 2017 saw vicious and crippling cyber-attacks across the globe, causing financial and reputational losses to the general public and businesses. Approximately 2.7 billion data records were stolen based on estimates of publicly reported incidents, which is twice the number of records stolen in 2016. The frequency of attacks and the stature of the victim enterprises are sending signals to escalate cybersecurity as a governance issue. Amongst the types of data stolen, there is a clear trend that customer information is the most sought-after target by hacking syndicates. Over 143 million customers were impacted by the Equifax breach, which occurred due to a vulnerability found in an open source software, allowing attackers to access sensitive files. During the first half of 2017, major breaches hit organizations in a variety of industries, exposing the records of millions of individuals. Our research indicates that even though 2015 and 2016 have seen some of the most successful breaches of high-value targets, the story has only gotten progressively worse.

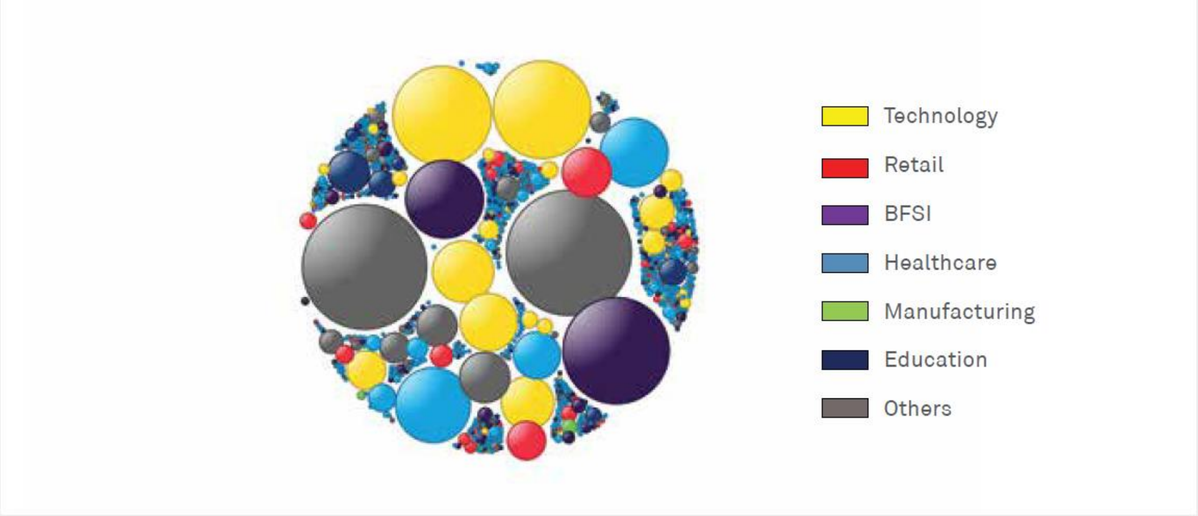


Fig. 6 Relative Impact of data breaches across various verticals (Larger the size of the bubble implies higher records were lost/stolen.)

In the above diagram the various verticals have been distributed as follows:

BFSI – Banking + Financial Services + Insurance + Professional Services

Healthcare – Healthcare + Hospitality

Retail – Retail + Social media + Entertainment

Manufacturing – Manufacturing + Industrial

Technology – Technology

Education – Education

Others – Government + Non-profit + Others

The increasing frequency of personal data breaches in organizations has impacted customer faith. For example, in July 2017, personal data of more than 14 million customers of a leading communications provider were exposed from an Amazon S3 storage server. The data contained names, PINs and phone numbers that could be used to access a customer's account.

The data breaches of 2017, from the standpoint of the number of records breached on a quarterly basis, is presented in Figure 2 as compared to the same period in 2016. As is evident, 2017 has seen a clear increase in the volume of data records lost. In fact, the number of records hypothetically stolen per second for 2017 has gone up to 88 per second from 43 per second as reported in 2016.

88 records were lost or stolen every second in 2017.

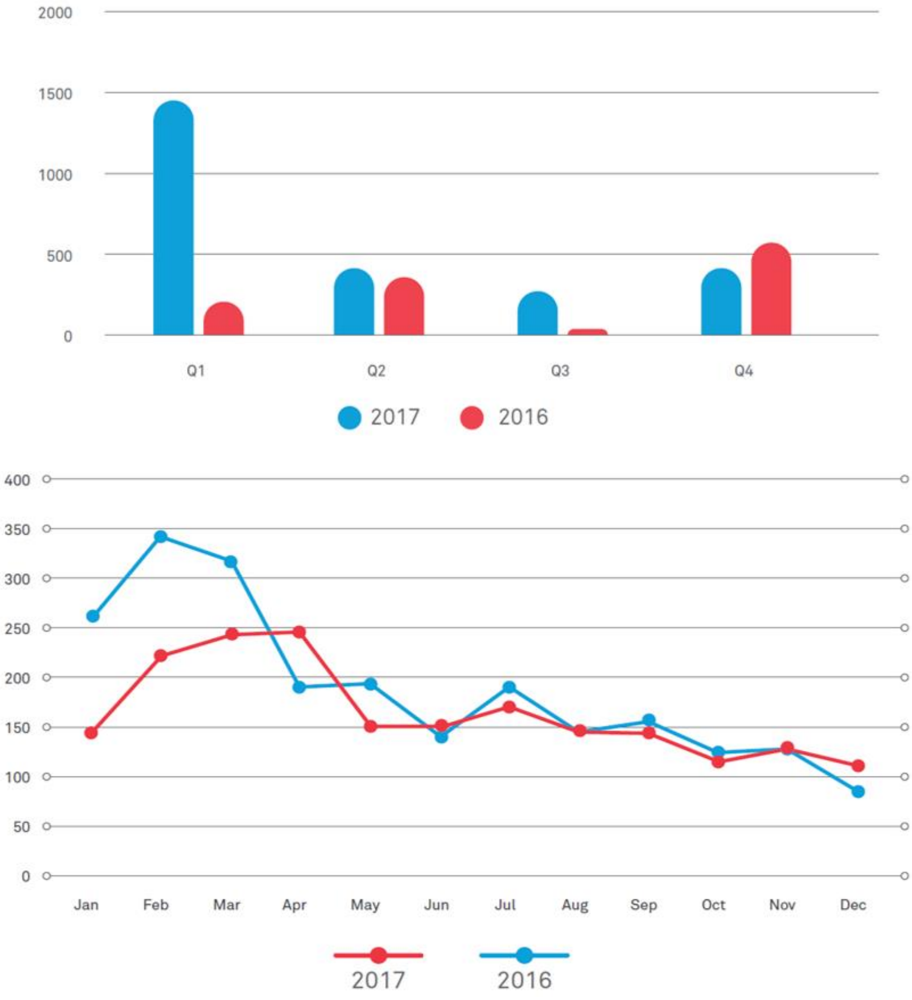


Fig. 7 Quarterly (Top) and Month-Wise (Bottom) distribution of breaches

When we compare the trends for the number of breaches per month in the last two years, a pattern can be observed in Figure 7. Both years saw escalating breaches occurring at the beginning of the year followed by a general reduction in the intensity of breaches. While Q1 witnessed the maximum volume of reported successful attacks, Q4 experienced the least in terms of distribution across the year. The percentage distribution across quarters was as follows: Q1:40%, Q2:23%, Q3:22%, Q4:15%. These statistics underscore the manifestation of cyber risks, historically. And with this increasing trend of attacks it is evident that enterprises across all verticals should invest more time and energy in safeguarding their information assets and the business processes they support.

2.1 Data Breaches Heat Map

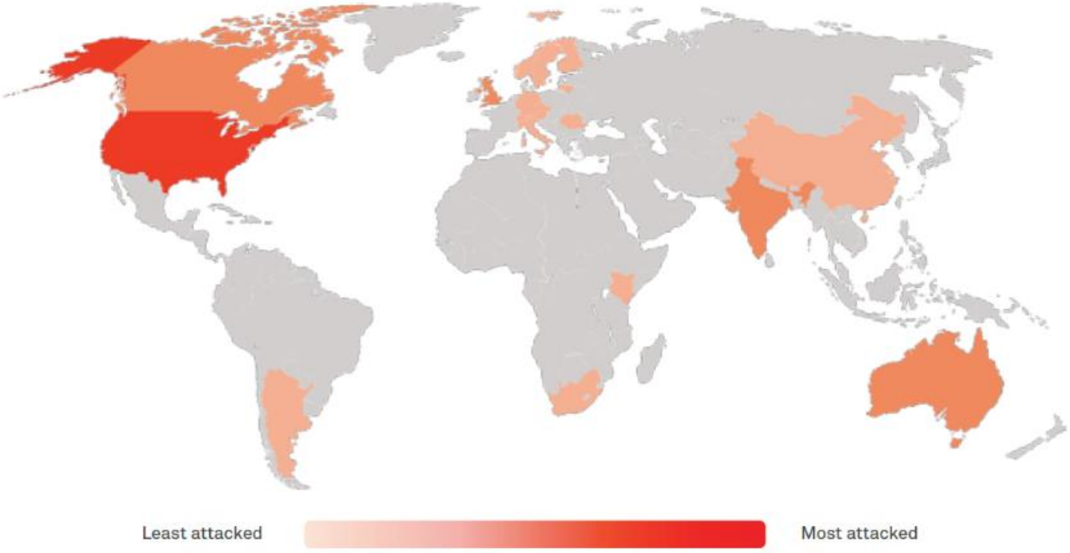


Fig. 8 Data Breaches by Geography (Year 2016)

The research on the data breaches of 2017 threw light on the geographical intensity of attacks over the course of the year. The analysis was done taking into account the victim destination based on the geographical location of business. Based on this analysis a global heat map was generated by Wipro. As is evident from the heat map in Figure 8, the US has suffered the maximum volume of attacks. The evidence of geographical distribution, found over time, strongly suggests that cyber-attacks are emerging as a global phenomenon, whose intensity and scale threatens every organization, irrespective of the sector, nationality or size. The data breaches heat map, as represented in Figure 8, hasn't changed much from 2016 in terms of the intensity of breaches experienced globally. The reasons behind this high concentration of attacks in certain countries can be attributed to different factors such as the presence of large corporations belonging to different industry verticals presenting attractive targets; geopolitical rivalries between countries leading to state-sponsored attacks; and strong breach notification law.

2.2 Quotable Quotes

“The only system which is truly secure is one which is switched off and unplugged, locked in a titanium safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn’t stake my life on it. “

In security matters,
there is nothing like **absolute security**”
“We are only trying to build **comfort levels,** because security costs money and lack of it costs much more”
“Comfort level is a manifestation of efforts as well as a realization of their effectiveness & limitations’

2.3 Definition

The security offered through online services to protect your online information in the cyberspace is part of a domain called cybersecurity.

Cyberspace: The global interdependent network of information technology infrastructures (both software and hardware), including the internet, tele communications networks, computer systems and embedded processors and controllers.

Cybersecurity in other words is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.

2.4 A Global Perspective

In 2016, almost half the world used the internet (3.5 billion users) & it is estimated that by 2020 there will be over 12 billion devices connected to the internet. 1 in 130 emails sent are malicious (2017 report by ITU or International Telecommunication Union). Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to USD 1 077, up from USD 294 a year earlier (+266%).

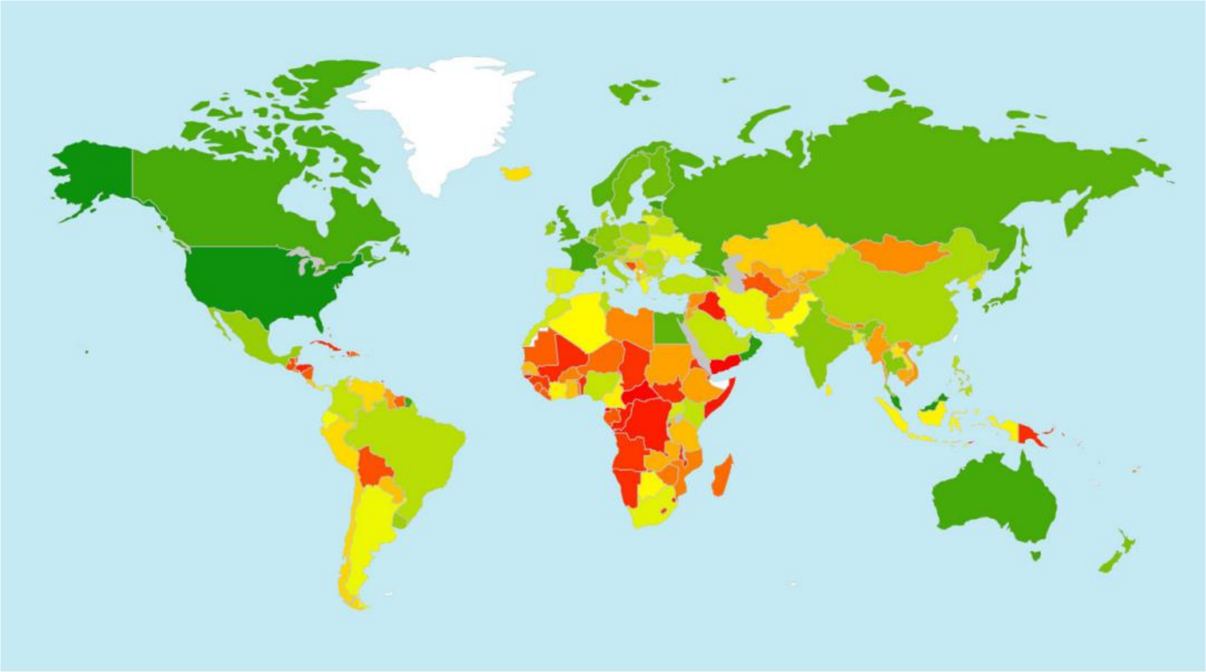


Fig. 9 GCI Heat Map (2017) published by ITU

India ranks 23d worldwide as per GCI and has a score of 0.683. Only 39% of respondents consider cybersecurity as a top concern. 46% of respondents across the Americas and 50% of the respondents in EMEA (Europe, the middle East and Africa) do not have a formal cybersecurity program. 76% of APAC (Asia Pacific) respondents indicated that they have a formal cybersecurity program. 50% of respondents indicated that hacktivists, organized crime, and employees – both current and former – are the sources of greatest cyber risk. 20% of respondents have not conducted a cybersecurity assessment, and only 25% of respondents provide cybersecurity training to employees at least annually.

20% of respondents who are required to have a cybersecurity program based on governmental, industry or customer requirements do not currently have a cybersecurity program. Limited time and budget along with a lack of qualified staff were the key reasons cited for not having an effective cybersecurity program.

More organizations that have a cybersecurity program reported experiencing a breach than those who do not have a formal cybersecurity program.

However, it is the organizations that have a cybersecurity program that are more likely to identify a breach. We are unable to report on the number of breaches that go undetected. The majority of the respondents indicated underinvestment in advanced cybersecurity initiatives such as a robust security incident response plan to identify, detect, and handle security incidents including data breaches.

2.5 How is the Indian Cyberspace changing?

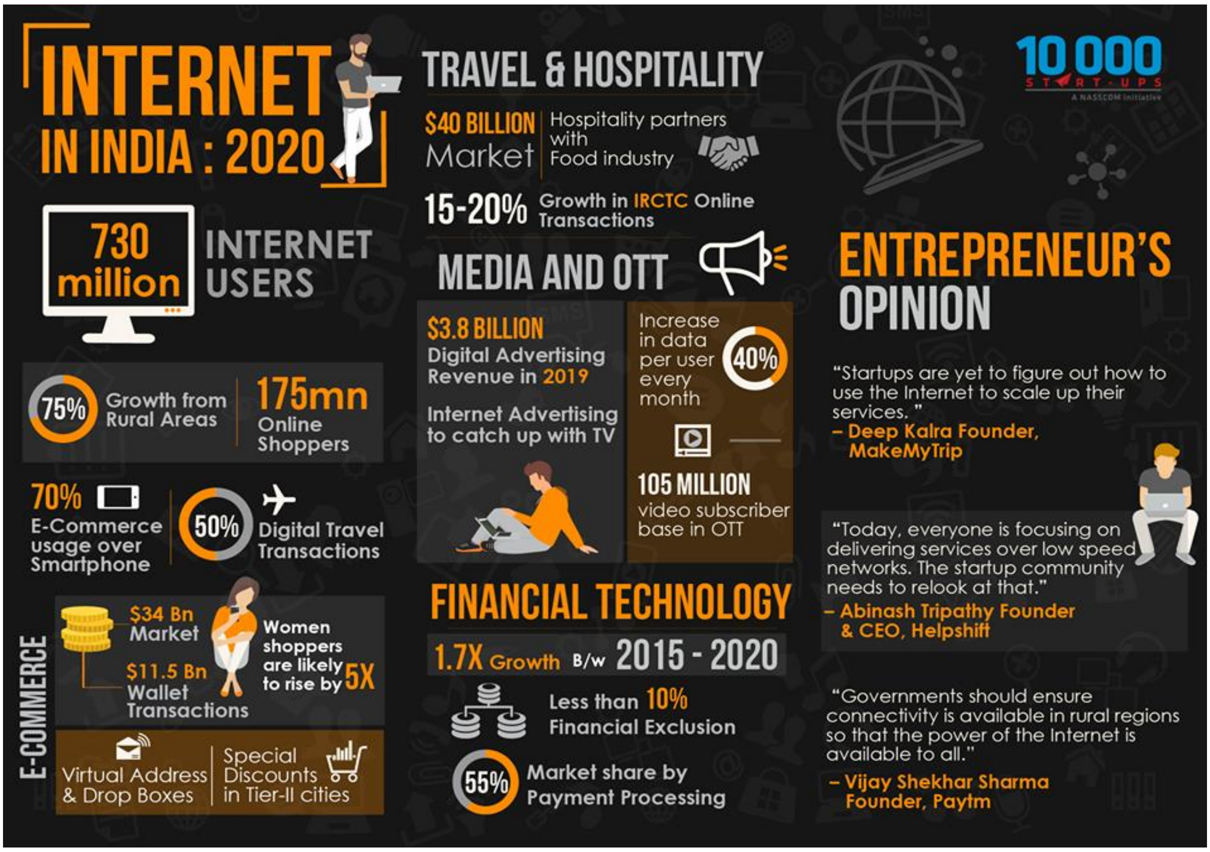

INTERNET IN INDIA : 2020
730 million INTERNET USERS
75% Growth from Rural Areas
175mn Online Shoppers
70% E-Commerce usage over Smartphone
50% Digital Travel Transactions
E-COMMERCE
$34 Bn Market
$11.5 Bn Wallet Transactions
Women shoppers are likely to rise by 5X
Virtual Address & Drop Boxes
Special Discounts in Tier-II cities
TRAVEL & HOSPITALITY
$40 BILLION Market
Hospitality partners with Food industry
15-20% Growth in IRCTC Online Transactions
MEDIA AND OTT
$3.8 BILLION Digital Advertising Revenue in 2019
Internet Advertising to catch up with TV
Increase in data per user every month 40%
105 MILLION video subscriber base in OTT
FINANCIAL TECHNOLOGY
1.7X Growth B/w 2015 - 2020
Less than 10% Financial Exclusion
55% Market share by Payment Processing
10 000 START-UPS A NASSCOM initiative
ENTREPRENEUR'S OPINION
"Startups are yet to figure out how to use the Internet to scale up their services."
– Deep Kalra Founder, MakeMyTrip
"Today, everyone is focusing on delivering services over low speed networks. The startup community needs to relook at that."
– Abinash Tripathy Founder & CEO, Helpshift
"Governments should ensure connectivity is available in rural regions so that the power of the Internet is available to all."
– Vijay Shekhar Sharma Founder, Paytm

Fig. 10 How will internet in India be in 2020?

2.6 Top 5 Myths about Cyber Security

1: I cannot be the target to criminals, only rich people and big organizations are.

India was the third worst-hit country in the recent WannaCry ransomware attacks. More than 40,000 computers were affected, but no major corporate or bank reported any disruption to their activities, raising doubts whether they are disclosing attacks at all.

2: Cyber Security! An IT issue.

Forbes states that; PEOPLE ARE OFTEN THE WEAKEST LINK IN THE SECURITY CHAIN. Though people and organizations are spending billions of dollars to protect themselves from the battle of cyber security yet safety starts from you.

3: I do not have important data in my PC therefore I cannot be a victim.

Cyber attackers not only look for the important data on the system but also trace all the online activities of an individual. The more we do and share online, the more we are vulnerable to cyber-attacks. It was reported in 2016 1 in 10 adults is the victim of fraud or online offences.

4: I only access safe locations and open e-mails from known sources, therefore I am safe.

This myth is a hoax among individuals, irrespective of the fact that phishing is the most common type of breach in the world. You would be surprised to know that 46,000 new phishing sites are created each day.

5: My passwords are enough to protect me.

Along with passwords you need to have extra layer of security to keep your data and yourself safe. Deloitte, one of the big four's and a leading source of cyber-security advice for corporates, has had it email server hacked using legit credentials, client details revealed, attackers on system for months and no 2FA.

2.7 Evolution of Cyber Threats

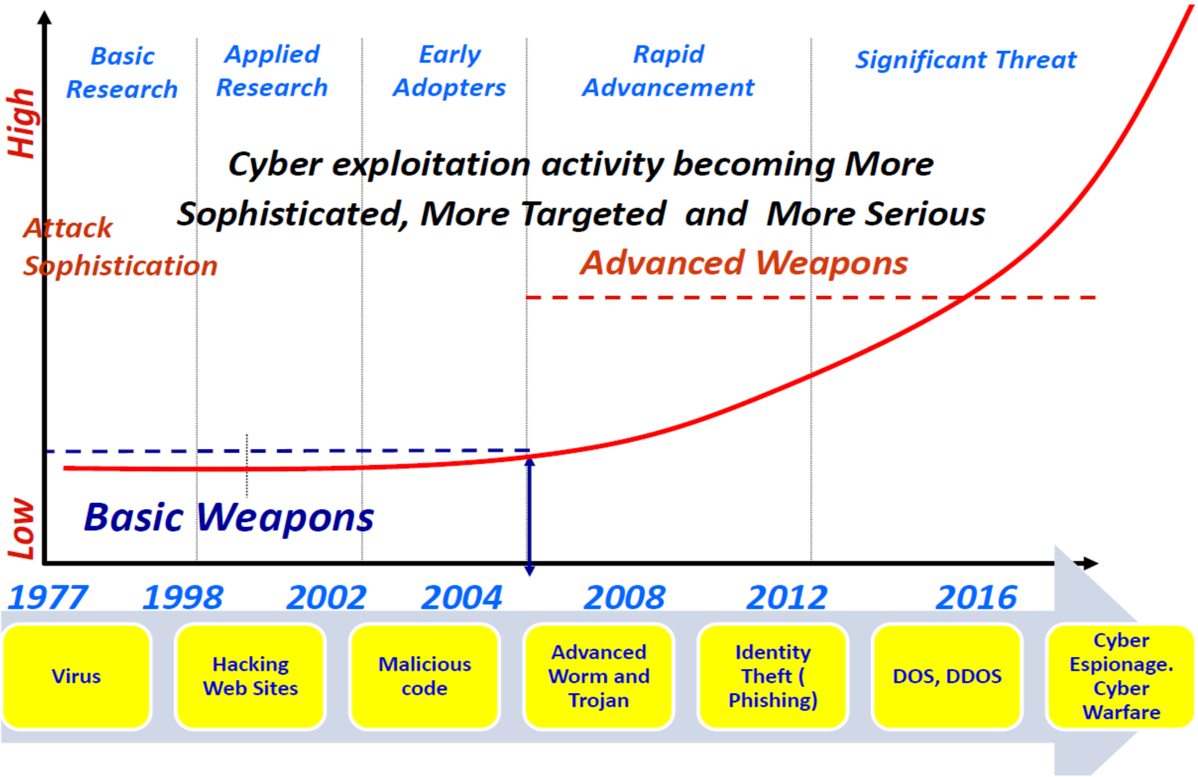


Fig. 11 Cyber Threat Evolution over the years (1977-2016)

2.8 Cyber Weapons spread across 2017

This section of the report aims to highlight the malware attacks detected and thwarted by CDCs across a sample set of multi-geographic environments in 2017. The incidents were de-identified and then analyzed for the malware threat type, relative distribution and growth across the four quarters of 2017. The analysis was carried out by sampling 9,700+ incidents to generate the insights.

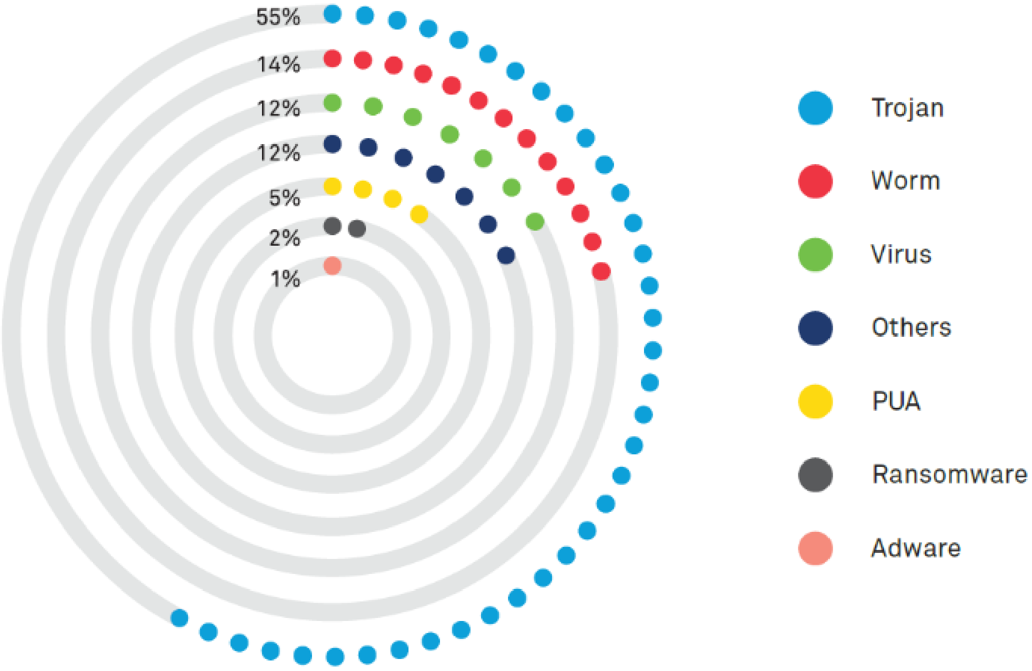


Fig. 12 Overall Malware Distribution in the year 2017

The above figure illustrates the percentage of different types of malware that were detected in 2017 across the following categories: Trojan, Virus, Worm, PUA, Adware and Ransomware. Trojans followed by worms and viruses occupy the top three positions across the various types detected.

2.9 The Ransomware Revolution

Holding your data to ransom is an easy way for an attacker to make a dishonest profit, and destroying data for other reasons such as a political agenda seems to be on the rise. The below mentioned are some measures that can actually reduce the risk across the board.

1. It is understandable that people choose to pay in the hope of getting their data back even though they know that this encourages the criminals. Before paying up, though, always check with your security software vendor:

- In case recovery may be possible without paying the ransom.
- In case it's known that paying the ransom won't or can't result in recovery for that particular ransomware variant.

2. Protecting your data proactively is safer than relying on the competence and good faith of the criminal. Back up everything that matters to you, often, by keeping at least some backups offline – to media that aren't routinely exposed to corruption by ransomware and other malware – in a physically secure location (preferably more than one location). And, obviously, backups defend against risks to data apart from ransomware and other malware, so should already be part of a disaster recovery plan.

3. Many people and organizations nowadays don't think of backup in terms of physical media like optical disks and flash storage, so much as in terms of some form of cloud storage. Which are very likely to be offsite, of course. Remember, however, where such storage is 'always on', its contents may be vulnerable to compromise by ransomware in the same way that local and other network-connected storage is. It's important that *offsite storage*:

- Is not routinely and permanently online
- Protects backed-up data from automatic and silent modification or overwriting by malware when the remote facility is online.
- Protects earlier generations of backed-up data from compromise so that even if disaster strikes the very latest backups, you can at least retrieve some data, including earlier versions of current data.
- Protects the customer by spelling out the provider's legal/contractual responsibilities, what happens if the provider goes out of business, and so on.

4. Don't underestimate the usefulness of backup media that aren't rewriteable/reusable. If you can't modify what's been written there, then neither can ransomware. Check every so often that your backup/recovery operation is (still) working properly and that your media (read-only, write-disabled, or write-enabled) are still readable (and that write-enabled media aren't routinely writeable). And back up your backups.

It is not right to say that you should rely on backups instead of using security software, but bear in mind that removing active ransomware with security software that detects ransomware is by no means the same as recovering data: removing the ransomware and then deciding to pay up means that the data may no longer be recoverable even with the cooperation of the criminals, because the decryption mechanism is part of the malware. On the other hand, you certainly don't want to restore your data to a system on which the ransomware is still active. Fortunately, safe backups can save your data if/when something malicious slips past your security software.

2.10 Critical Infrastructure Attacks on the rise

Cyber threats to critical infrastructure jumped into the headlines in 2017, starting with a Reuters report in January that a recent power outage in Ukraine "was a cyber-attack". In late December of 2015, cyberattacks on Ukrainian power companies resulted in electricity service being turned off for several hours to hundreds of thousands of homes in that part of the world. The first article published by ESET researchers in 2016 (on this incident) was Anton Cherepanov's analysis of Black Energy, the malicious code used in that cyberattack. That specific malware did not directly manipulate Industrial Control System (ICS) devices, but it enabled hackers to penetrate the networks of electricity distribution companies and kill software used by ICS equipment. Press reports then – some with eye-grabbing headlines like "Malware turns off the lights" – did not make that distinction clear.

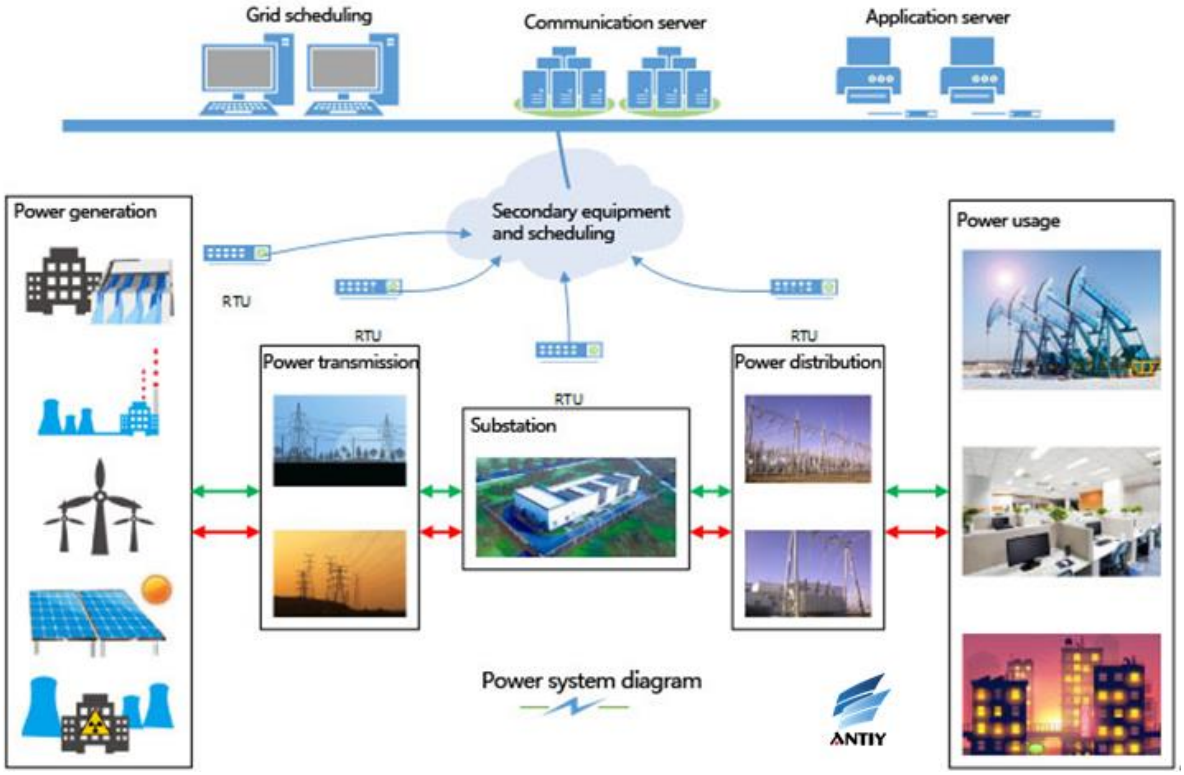


Fig. 13 Ukraine Power System Architecture

Of course, many of the organizations that currently operate critical infrastructure are working hard to secure it. ESET’s research further suggests that any future cyberattack using Industroyer (Malware Framework) would need to be tailored to specific targets. This may limit eventual outbreaks to well-funded attackers and impede widespread campaigns aimed at turning out the lights, crippling transportation, or halting critical manufacturing. However, it is not unusual for such conditions to change.

The industrial equipment that Industroyer targeted is widely used well beyond Ukraine – for example in the UK, EU, and the US – and across multiple critical sectors. Critical Infrastructure attacks on the rise over time as attack code is refined and intelligence is gathered. In other words, the ability to carry out cyberattacks on the power grid will tend to increase through 2018 unless blocked by preemptive measures, like system upgrades, early detection of network probing, and drastic improvement in phishing detection and avoidance.

While many large companies appear to be taking cybersecurity much more seriously these days, with security teams getting both the budget and the C-level backing required to do a good job, many smaller businesses supplying goods and services to larger organizations are struggling. That makes them an attractive target if, for example, they happen to have a blockbuster sitting on their post-production audio processing systems, which happen to be connected to their office network, and whose users have not been trained to recognize phishing emails.

Critical infrastructure organizations need to keep improving their security in 2018, reducing the effectiveness of phishing attacks (still amongst the most prevalent attack vectors), segregating and controlling network access, reviewing and testing both old and new hardware and software, and doing digital due diligence on suppliers. They also need to watch for and react to the kind of network probing and surveillance that may presage a full-on cyberattack.

2.11 Police and malware research join forces

The primary purpose of malware analysis is to determine how a given piece of malware works, extract IOCs (Indicators of Compromise) and determine potential countermeasures. This work is almost purely technical in nature: it focuses on binary files and their properties. Results from malware analysis are crucial for organisations to allow them to defend against an outbreak or to remediate a live infiltration. They are also crucial for security software vendors, enabling them to build better detections and protective measures for their customers.

Case Study of Disruption campaign against Dorkbot:

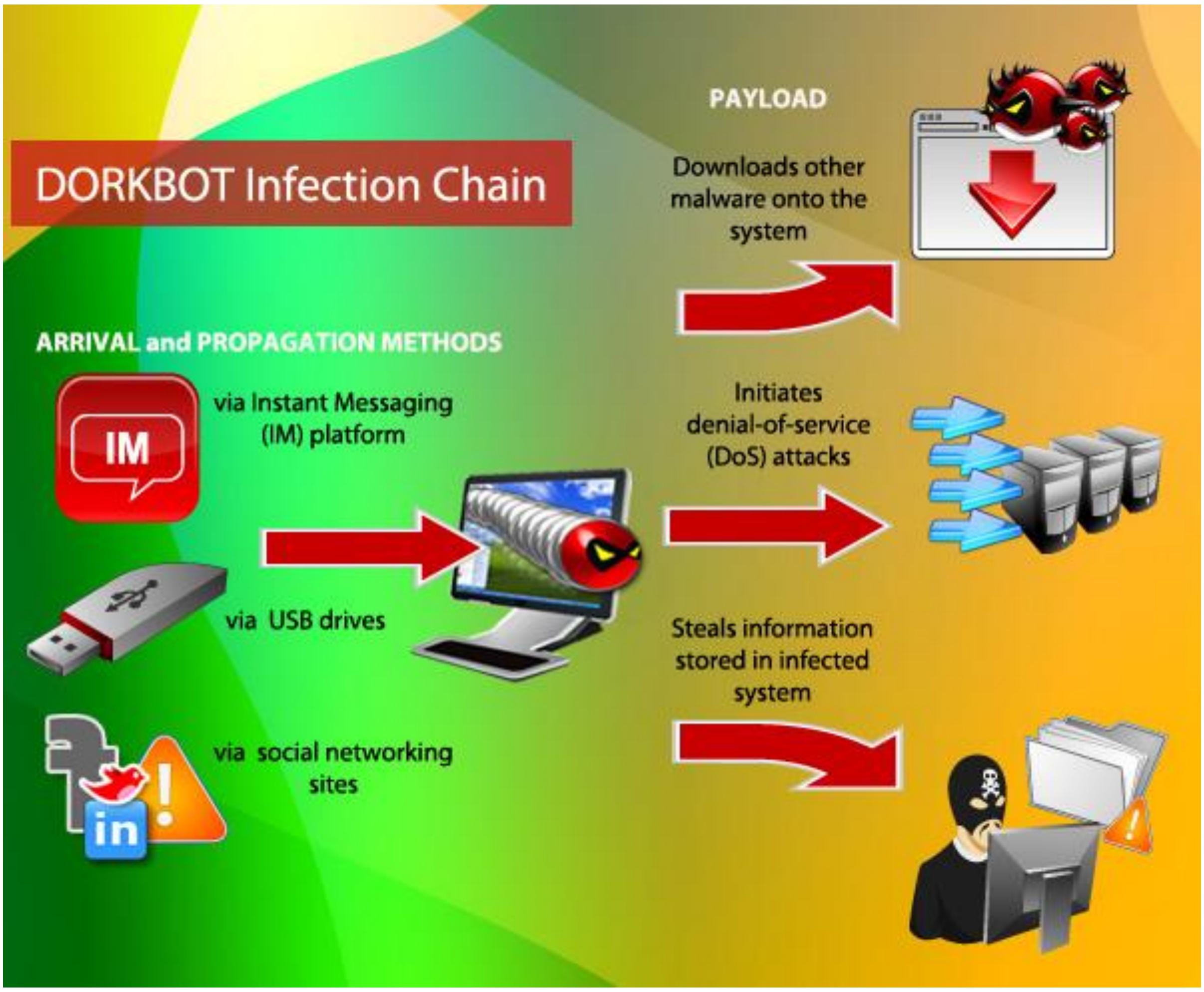

DORKBOT Infection Chain
ARRIVAL and PROPAGATION METHODS
IM
via Instant Messaging (IM) platform
via USB drives
via social networking sites
in
PAYLOAD
Downloads other malware onto the system
Initiates denial-of-service (DoS) attacks
Steals information stored in infected system

Fig. 14 How the 'Dorkbot Malware' spreads across users

The primary purpose of malware analysis is to determine how a given piece of malwareworks, extract IOCs (Indicators of Compromise) and determine potential countermeasures. This work is almost purely technical in nature: it focuses on binary files and their properties. Results from malware analysis are crucial for organisations to allow them to defend againstan outbreak or to remediate a live infiltration. They are also crucial for security software vendors, enabling them to build better detections and protective measures for their customers.

In 2015, ESET was invited to join Microsoft's Coordinated Malware Eradication campaign (CME) against the Win32/Dorkbot malware family. Dorkbot was a kit, available for sale in underground forums, that infected over one million PCs spanning multiple, independent botnets. The objective of this CME campaign was to massively disrupt as many of those botnets as possible by taking down the related C&C infrastructures simultaneously.

In support of this operation, ESET malware researchers automated the process of extracting C&C information from Dorkbot binaries. This process was applied to the flow of both existing and new Dorkbot samples. Then the results were manually sanitized by removing known sinkholes and cleaning domains/IPs to mitigate the risk of taking down legitimate resources.

Microsoft merged that information with their own data to create an exhaustive list of all the active C&C nodes to target. This complete list was then relayed to law enforcement agencies all around the world, such as the Canadian Radio-television and Telecommunications Commission (CRTC), the Department of Homeland Security's United States Computer Emergency Readiness Team (DHS/US CERT), Europol, the Federal Bureau of Investigation (FBI), Interpol, and the Royal Canadian Mounted Police (RCMP). On disruption day, warrants and takedown notices were executed in a coordinated maneuver. Since then, a sharp decline in Dorkbot activity has been noticed worldwide, indicating that the CME campaign succeeded.

Some people think the reason so few cybercrimes go punished is that it is easy to perform criminal activities on the internet anonymously, without much chance of being traced. It is actually pretty much the opposite: maintaining perfect operational security (OPSEC) consistently is pretty hard. Some people also give up going after cybercriminals because even when identified, cybercriminals remain out of reach.

Maybe they live in a jurisdiction that has no effective laws against cybercrime, or that has no mutual extradition treaty with the countries investigating them? But there again, humans make mistakes. All it might take to be caught is for a known cybercriminal to leave his country to take some vacation time abroad.

2017 has been marked by a large number of arrests in various cybercrime operations, as outlined in Stephen Cobb's excellent summary. As major law enforcement entities gain experience in working with private entities such as ESET to track cybercriminals, we can predict with some confidence that 2018 will bring more and more successful investigations that will contribute to making the internet a safer place for everyone. Except for cybercriminals.

2.12 Can Electoral Processes be protected?

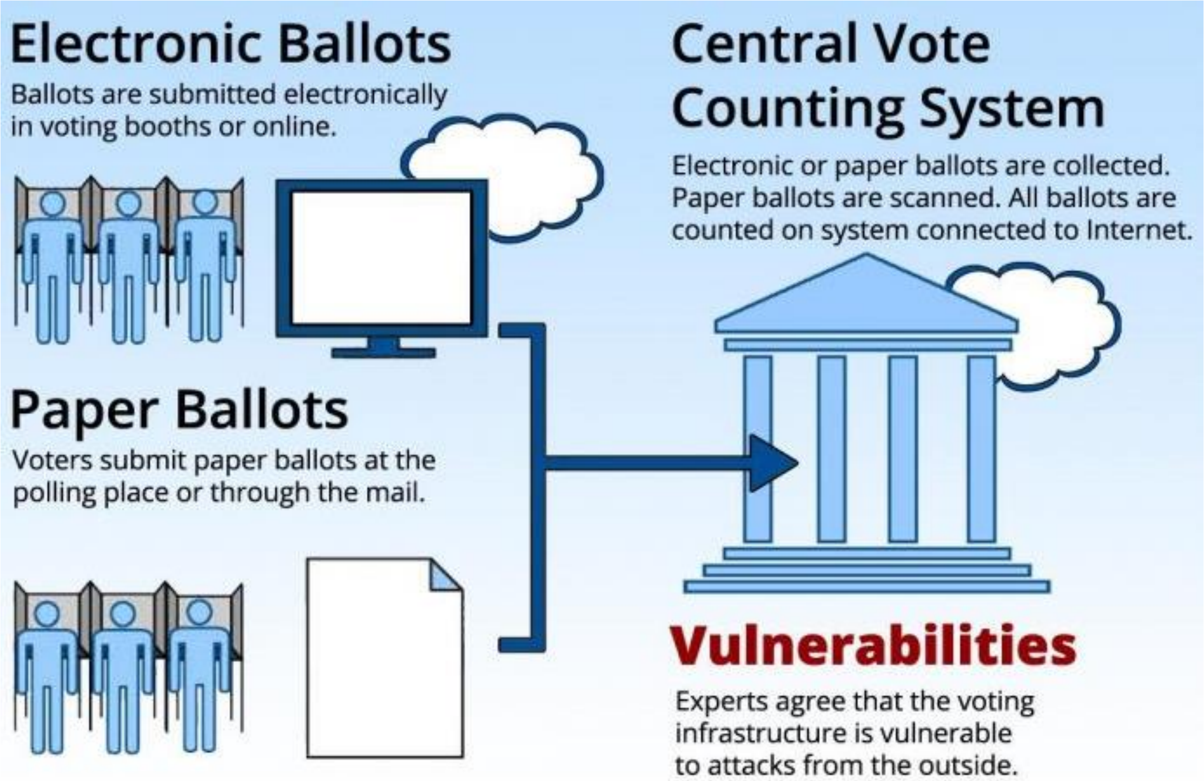

Electronic Ballots
Ballots are submitted electronically in voting booths or online.
Central Vote Counting System
Electronic or paper ballots are collected. Paper ballots are scanned. All ballots are counted on system connected to Internet.
Paper Ballots
Voters submit paper ballots at the polling place or through the mail.
Vulnerabilities
Experts agree that the voting infrastructure is vulnerable to attacks from the outside.

Fig. 15 How is the Voting System vulnerable to outside attacks?

Back in 2006, Finnish computer programmer and co-founder of ROMmon (Harri Hursti) had already demonstrated, how the Diebold voting system in Leon County, Florida, could be easily and completely compromised just by using a memory card.

Just like that, he was able to change all of the votes without being detected. Nonetheless, this same software – that with just a few adjustments, a new name and a change of ownership – continues to be used in the United States to record and count tally votes.

Brazil's electronic ballot box has been mired in controversy since 2012, when it was discovered that it was possible to crack voting secrecy completely. After years of substantiated allegations of vulnerabilities, the Superior Electoral Court will go back to implementing paper ballots (in a hybrid format) for just 5% of ballot boxes to be used for elections in 2018. Meanwhile, electronic ballot procedures in both Argentina and Germany have been shown to be flawed as well.

Firstly, the influence of social networks on public opinion, especially in respect to pushing a political agenda, particularly the way in which they support hacktivism; and lastly, the need to include national cybersecurity issues as part of the political agenda.

2.13 Personal Data in this new age of Technology and Legislation

Free Software and Services:

As consumers expect to enjoy software at no cost, or very low cost, some vendors have taken the decision to enter the data-collection and data-sharing business. Providers of free software only have a few methods by which to monetize their products and the least intrusive, at least from the perspective of what the end user actually sees, could be the collection and sale of data to third parties.

The free or low-cost cybersecurity software will continue trending over the next year. This will increase risks connected with data privacy, as free software usually lacks traditional monetization methods, and instead, introduces complex disclosure statements that are in part designed to obscure intent as to what data is being collected and whether it can be sold. This is evidenced by the

Personal data in the new age of technology and legislation many companies offering lengthy and unreadable privacy policies that are only comprehensible to lawyers.

“With any free product it is important to understand how the company is making money.”

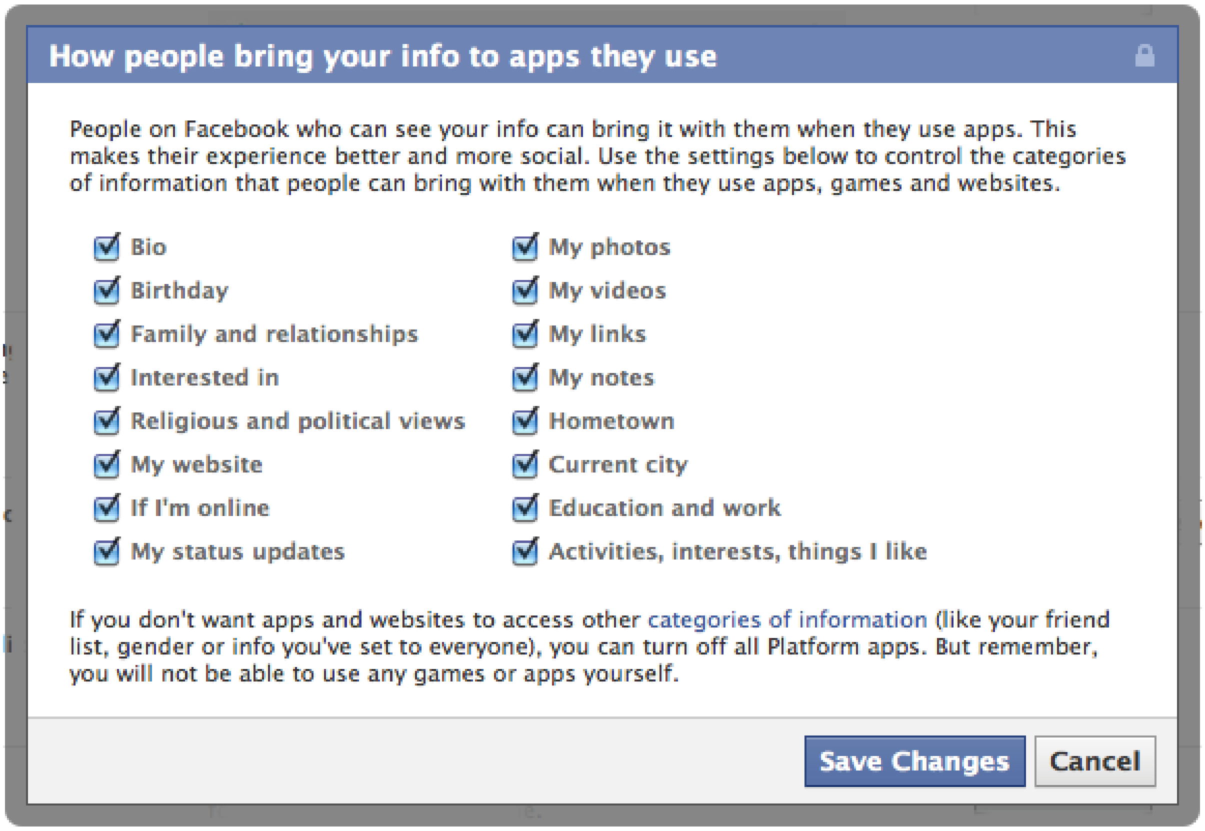
Internet of Things:

As you drive home from work, your phone is transmitting traffic conditions to share with other drivers, hopefully allowing you to make intelligent detours or driving decisions to get you home earlier. The connected thermostat at home is communicating with your phone, relaying your location and the time of day. Currently, you are homeward bound. As you enter the suburban street where you live, the garage door opens automatically, using your proximity to make a decision. The lights come on and your current choice of music transfers from the car to your home automatically. IoT devices are designed to work together, simplifying our existence.

And every device can tell a story via the data it collects. Combining those various data streams, any attacker will be able to paint a full picture of your life: where we work, where we eat, when we go to the gym, what cinema we visit, where we shop and so on. The combination of this data and advances in machine learning and artificial intelligence could mean that we start becoming puppets of technology as it increasingly makes decisions for all of us.

Legislation:

“Every time a device asks to be connected we need to educate the end user to read the privacy policy and to make informed decisions about whether or not to accept the data collection terms as set out in the privacy policy”.



How people bring your info to apps they use

People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.

☑ Bio
☑ Birthday
☑ Family and relationships
☑ Interested in
☑ Religious and political views
☑ My website
☑ If I'm online
☑ My status updates
☑ My photos
☑ My videos
☑ My links
☑ My notes
☑ Hometown
☑ Current city
☑ Education and work
☑ Activities, interests, things I like

If you don't want apps and websites to access other categories of information (like your friend list, gender or info you've set to everyone), you can turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.

Fig. 16 Categories of information accessed by apps, websites and games on Facebook

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email id not "legal" in our country. There is no law in the country, which gives legal validity, and sanction to email.

It should be the duty of the three stake holders viz. i) the rulers, regulators, law makers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.

3. THE DEFENCE LANDSCAPE

These are some interesting insights and findings from the survey conducted with CISOs about the state of security management and governance, data security, application security, network security, endpoint security, security monitoring and analytics, cloud security and IOT security in enterprises:

Are the boardrooms listening?

4% was the maximum share of overall enterprise IT budget allocated for security in 2017 as per 39% of the organizations in 2017

If it’s not on the RADAR, no one will see it coming!

Only 36% of organizations tracked how much of the IT estate/asset base was effectively monitored by their SOC

Protect the keys to your kingdom

29% of organizations ranked PAM (Privileged Access Management) as their first choice amongst data security controls

Applications are the soft underbelly

Only 21% of the organizations were doing security assessment of business-critical applications for every application build/release cycle

Are you ready for the DDoS garden hose?

45% of organizations faced some form of DDoS attack in 2017

Users are still the weak link

60% of organizations ranked phishing emails as the primary vector of endpoint attack

Serverless computing cannot be security less!

44% of organizations polled minimal control of security as the main hurdle preventing them from migrating applications to a Serverless model (FaaS – Function as a Service)

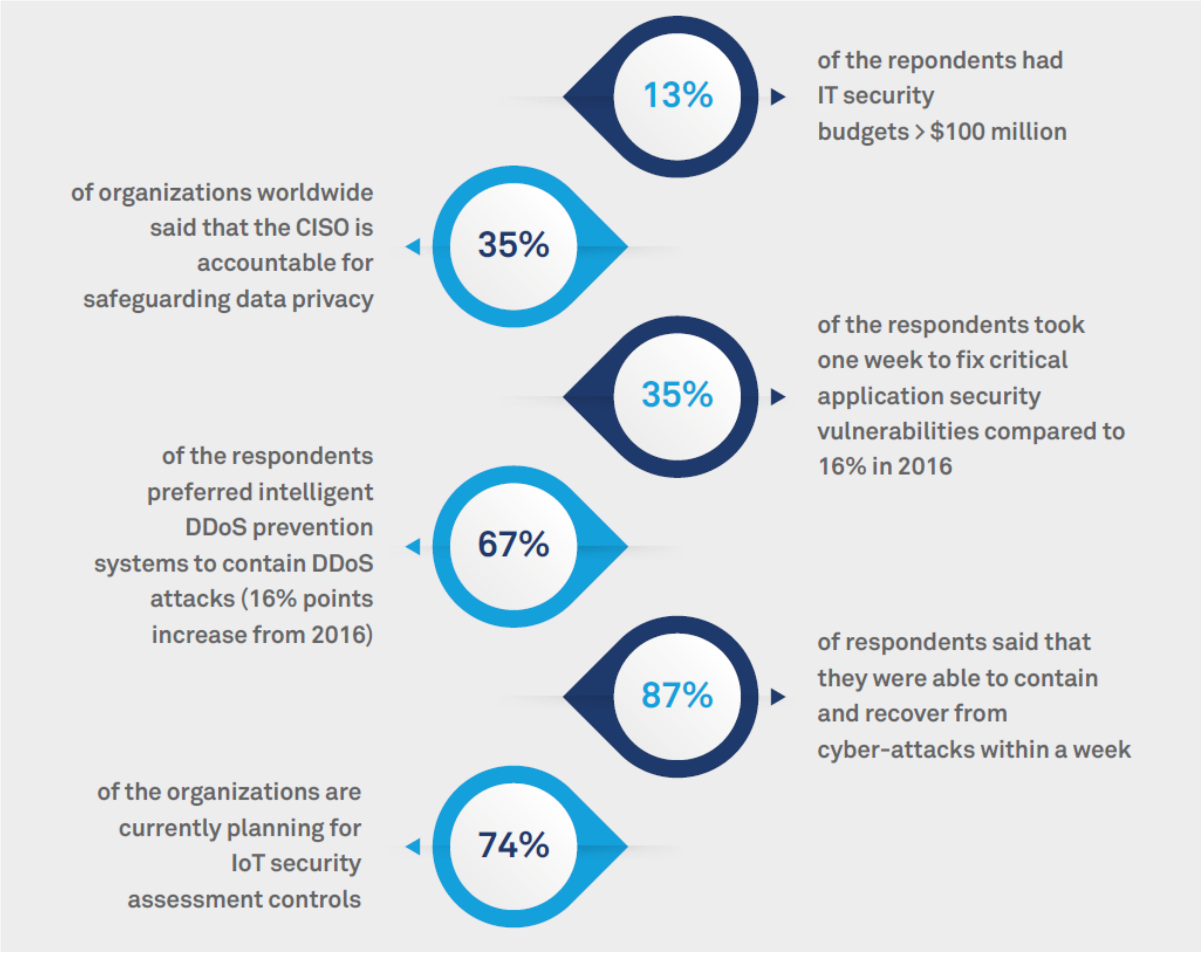


Fig. 17 Other insights from the survey conducted with CISO's about Cyber Security

How can we as citizens keep ourselves Cyber Safe?

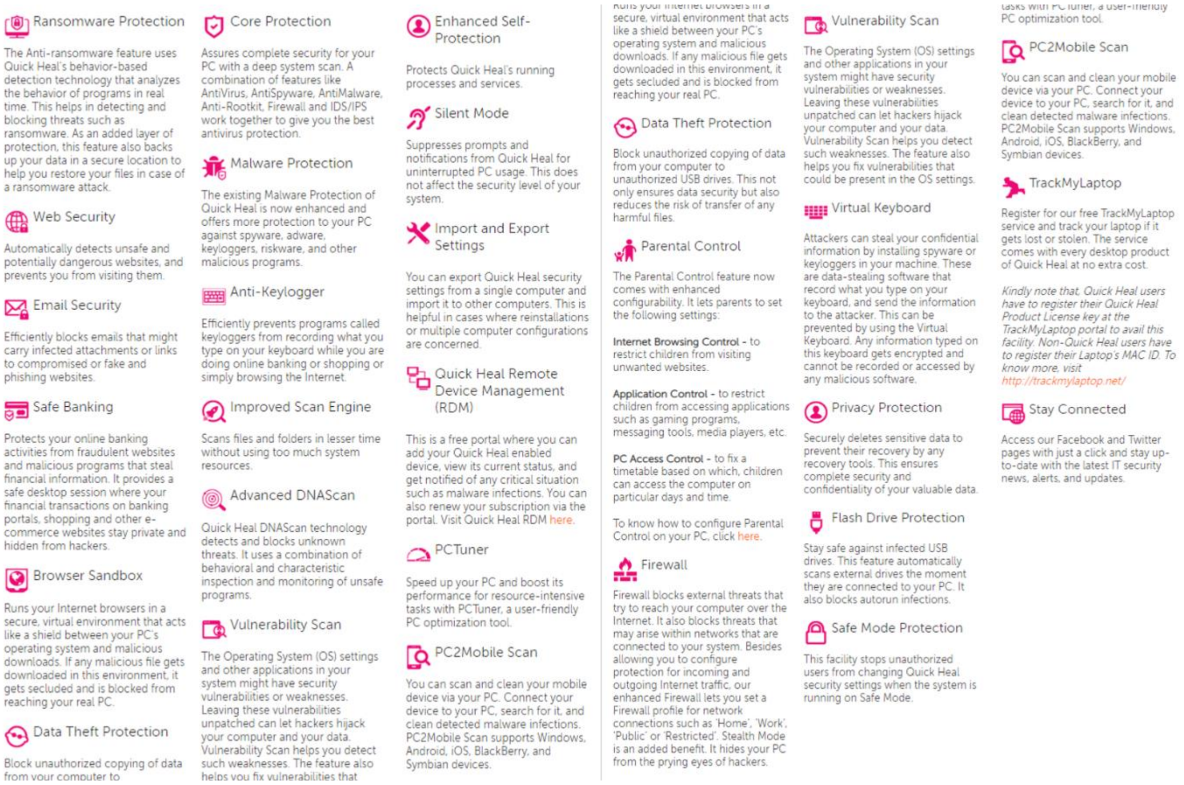
1. Use Anti-Virus Software and keep it up to date.

The software is designed to protect your computer against known viruses but, with new viruses emerging daily, anti-virus programs need regular updates. Check with the website of your anti-virus software company to see sample descriptions of viruses and to get regular updates for your software. You should do updates on your computer every other day. (Set auto update in the settings)

Can we completely rely on Windows Defender?

Unfortunately, Windows Defender (Windows Anti Malware Product) has at least two major disadvantages.

- First, my own experience has been that Defender doesn't do as good of a job of detecting malware as some other products on the market. Defender is great for removing infections, but only if those infections can be detected.
- The other problem with Defender is that some malware is specifically designed to attack and disable it / scan speed is slow / ability to detect threats is not very impressive.



Ransomware Protection

The Anti-ransomware feature uses Quick Heal's behavior-based detection technology that analyzes the behavior of programs in real time. This helps in detecting and blocking threats such as ransomware. As an added layer of protection, this feature also backs up your data in a secure location to help you restore your files in case of a ransomware attack.

Web Security

Automatically detects unsafe and potentially dangerous websites, and prevents you from visiting them.

Email Security

Efficiently blocks emails that might carry infected attachments or links to compromised or fake and phishing websites.

Safe Banking

Protects your online banking activities from fraudulent websites and malicious programs that steal financial information. It provides a safe desktop session where your financial transactions on banking portals, shopping and other e-commerce websites stay private and hidden from hackers.

Browser Sandbox

Runs your Internet browsers in a secure, virtual environment that acts like a shield between your PC's operating system and malicious downloads. If any malicious file gets downloaded in this environment, it gets secluded and is blocked from reaching your real PC.

Data Theft Protection

Block unauthorized copying of data from your computer to

Core Protection

Assures complete security for your PC with a deep system scan. A combination of features like AntiVirus, AntiSpyware, AntiMalware, Anti-Rootkit, Firewall and IDS/IPS work together to give you the best antivirus protection.

Malware Protection

The existing Malware Protection of Quick Heal is now enhanced and offers more protection to your PC against spyware, adware, keyloggers, riskware, and other malicious programs.

Anti-Keylogger

Efficiently prevents programs called keyloggers from recording what you type on your keyboard while you are doing online banking or shopping or simply browsing the Internet.

Improved Scan Engine

Scans files and folders in lesser time without using too much system resources.

Advanced DNAScan

Quick Heal DNAScan technology detects and blocks unknown threats. It uses a combination of behavioral and characteristic inspection and monitoring of unsafe programs.

Vulnerability Scan

The Operating System (OS) settings and other applications in your system might have security vulnerabilities or weaknesses. Leaving these vulnerabilities unpatched can let hackers hijack your computer and your data. Vulnerability Scan helps you detect such weaknesses. The feature also helps you fix vulnerabilities that

Enhanced Self-Protection

Protects Quick Heal's running processes and services.

Silent Mode

Suppresses prompts and notifications from Quick Heal for uninterrupted PC usage. This does not affect the security level of your system.

Import and Export Settings

You can export Quick Heal security settings from a single computer and import it to other computers. This is helpful in cases where reinstallations or multiple computer configurations are concerned.

Quick Heal Remote Device Management (RDM)

This is a free portal where you can add your Quick Heal enabled device, view its current status, and get notified of any critical situation such as malware infections. You can also renew your subscription via the portal. Visit Quick Heal RDM here.

PCTuner

Speed up your PC and boost its performance for resource-intensive tasks with PCTuner, a user-friendly PC optimization tool.

PC2Mobile Scan

You can scan and clean your mobile device via your PC. Connect your device to your PC, search for it, and clean detected malware infections. PC2Mobile Scan supports Windows, Android, iOS, BlackBerry, and Symbian devices.

Runs your Internet browsers in a secure, virtual environment that acts like a shield between your PC's operating system and malicious downloads. If any malicious file gets downloaded in this environment, it gets secluded and is blocked from reaching your real PC.

Data Theft Protection

Block unauthorized copying of data from your computer to unauthorized USB drives. This not only ensures data security but also reduces the risk of transfer of any harmful files.

Parental Control

The Parental Control feature now comes with enhanced configurability. It lets parents to set the following settings:

Internet Browsing Control - to restrict children from visiting unwanted websites.

Application Control - to restrict children from accessing applications such as gaming programs, messaging tools, media players, etc.

PC Access Control - to fix a timetable based on which, children can access the computer on particular days and time.

To know how to configure Parental Control on your PC, click here.

Firewall

Firewall blocks external threats that try to reach your computer over the Internet. It also blocks threats that may arise within networks that are connected to your system. Besides allowing you to configure protection for incoming and outgoing Internet traffic, our enhanced Firewall lets you set a Firewall profile for network connections such as 'Home', 'Work', 'Public' or 'Restricted'. Stealth Mode is an added benefit. It hides your PC from the prying eyes of hackers.

Vulnerability Scan

The Operating System (OS) settings and other applications in your system might have security vulnerabilities or weaknesses. Leaving these vulnerabilities unpatched can let hackers hijack your computer and your data. Vulnerability Scan helps you detect such weaknesses. The feature also helps you fix vulnerabilities that could be present in the OS settings.

Virtual Keyboard

Attackers can steal your confidential information by installing spyware or keyloggers in your machine. These are data-stealing software that record what you type on your keyboard, and send the information to the attacker. This can be prevented by using the Virtual Keyboard. Any information typed on this keyboard gets encrypted and cannot be recorded or accessed by any malicious software.

Privacy Protection

Securely deletes sensitive data to prevent their recovery by any recovery tools. This ensures complete security and confidentiality of your valuable data.

Flash Drive Protection

Stay safe against infected USB drives. This feature automatically scans external drives the moment they are connected to your PC. It also blocks autorun infections.

Safe Mode Protection

This facility stops unauthorized users from changing Quick Heal security settings when the system is running on Safe Mode.

tasks with PCTuner, a user-friendly PC optimization tool.

PC2Mobile Scan

You can scan and clean your mobile device via your PC. Connect your device to your PC, search for it, and clean detected malware infections. PC2Mobile Scan supports Windows, Android, iOS, BlackBerry, and Symbian devices.

TrackMyLaptop

Register for our free TrackMyLaptop service and track your laptop if it gets lost or stolen. The service comes with every desktop product of Quick Heal at no extra cost.

Kindly note that, Quick Heal users have to register their Quick Heal Product License key at the TrackMyLaptop portal to avail this facility. Non-Quick Heal users have to register their Laptop's MAC ID. To know more, visit http://trackmylaptop.net/

Stay Connected

Access our Facebook and Twitter pages with just a click and stay up-to-date with the latest IT security news, alerts, and updates.

Fig. 18 Additional features provided by paid antivirus software such as Quick Heal

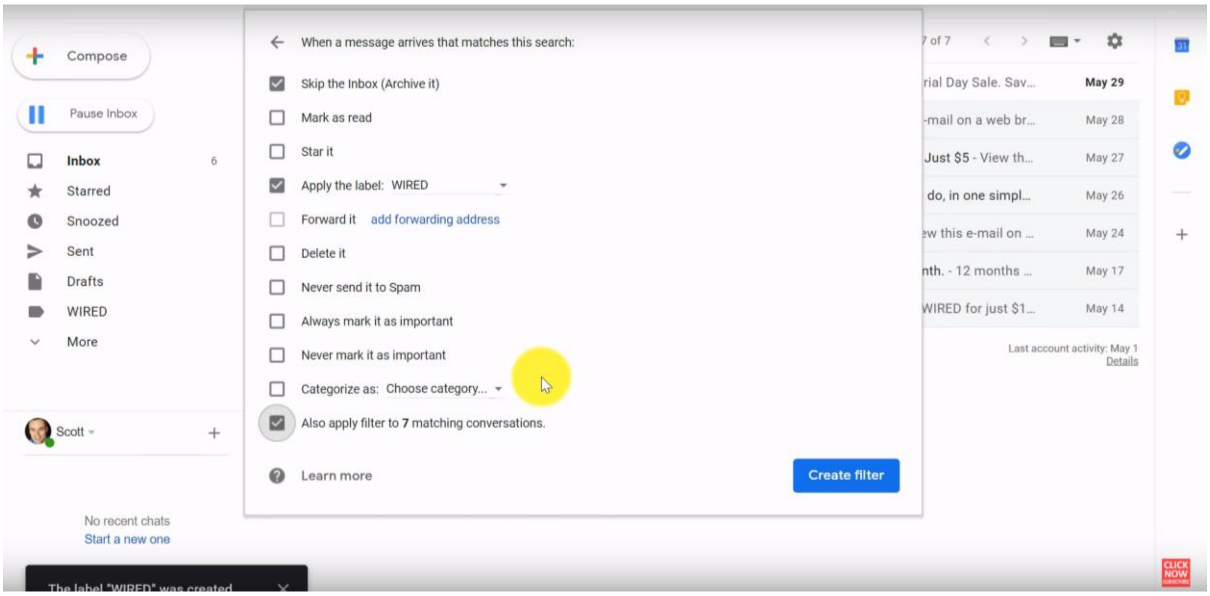
2. Don't open e-mails or attachments from unknown sources.

Be suspicious of any unexpected e-mail attachments even if they appear to be from someone you know. If you receive a suspicious e-mail, the best thing to do is to delete the entire message including its attachments. For example, you could also use email filters for pre delivery message scanning.

E.g. You can manage your incoming mail using Gmail's filters to send email to a label, or archive, delete, star, or automatically forward your mail. Below are some of the things you can do:

- Enhance security for forged spam

- Email Whitelists and Blacklists
- Allow or deny certain IP addresses in Gmail
- Create Spam Filters and customize them
- Check if your Gmail message is authenticated?
- Set up an inbound email gateway
- Use enhanced pre-delivery message scanning
- Set options for non-Gmail mailbox users
- Set guidelines for Bulk Senders of emails



When a message arrives that matches this search:

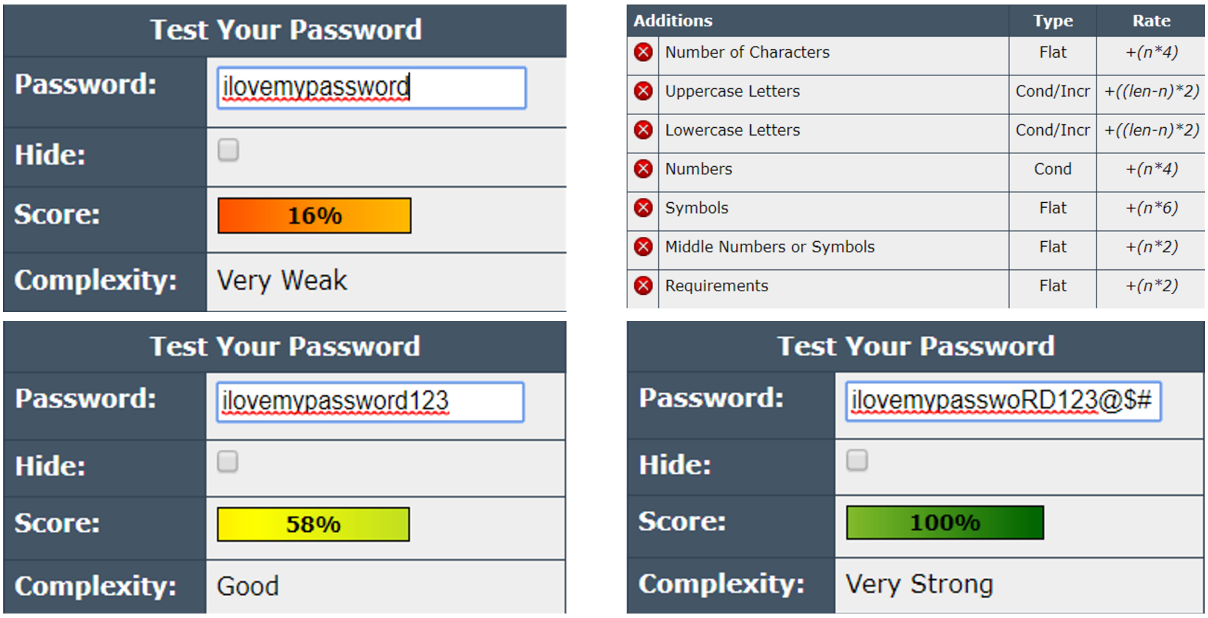
☑ Skip the Inbox (Archive it)
☐ Mark as read
☐ Star it
☑ Apply the label: WIRED
☐ Forward it add forwarding address
☐ Delete it
☐ Never send it to Spam
☐ Always mark it as important
☐ Never mark it as important
☐ Categorize as: Choose category...
☑ Also apply filter to 7 matching conversations.

Compose
Pause Inbox
Inbox 6
Starred
Snoozed
Sent
Drafts
WIRED
More
Scott
No recent chats
Start a new one
The label "WIRED" was created
Learn more
Create filter
7 of 7
rial Day Sale. Sav... May 29
-mail on a web br... May 28
Just $5 - View th... May 27
do, in one simpl... May 26
ew this e-mail on ... May 24
nth. - 12 months ... May 17
WIRED for just $1... May 14
Last account activity: May 1
Details
CLICK NOW

Fig. 19 Creating a Gmail Filter

3. Choose Strong Passwords.

Passwords are one of the biggest weak spots in the whole Internet security structure, but there's currently no way around them. And the problem with passwords is that people tend to choose easy ones to remember (such as "password" and "123456"), which are also easy for cyber thieves to guess. Select strong passwords that are harder for cybercriminals to demystify. Password manager software can help you to manage multiple passwords so that you don't forget them. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters. You could use a ‘Password Manager’ to store and organize your passwords.



Test Your Password	
Password:	ilovemypassword
Hide:	□
Score:	16%
Complexity:	Very Weak

	Additions	Type	Rate
☒	Number of Characters	Flat	+(n*4)
☒	Uppercase Letters	Cond/Incr	+((len-n)*2)
☒	Lowercase Letters	Cond/Incr	+((len-n)*2)
☒	Numbers	Cond	+(n*4)
☒	Symbols	Flat	+(n*6)
☒	Middle Numbers or Symbols	Flat	+(n*2)
☒	Requirements	Flat	+(n*2)

Test Your Password	
Password:	ilovemypassword123
Hide:	□
Score:	58%
Complexity:	Good

Test Your Password	
Password:	ilovemypasswoRD123@$#
Hide:	□
Score:	100%
Complexity:	Very Strong

Fig. 20 How to choose a strong password

4. Enable Multi Factor Authentication on your accounts.

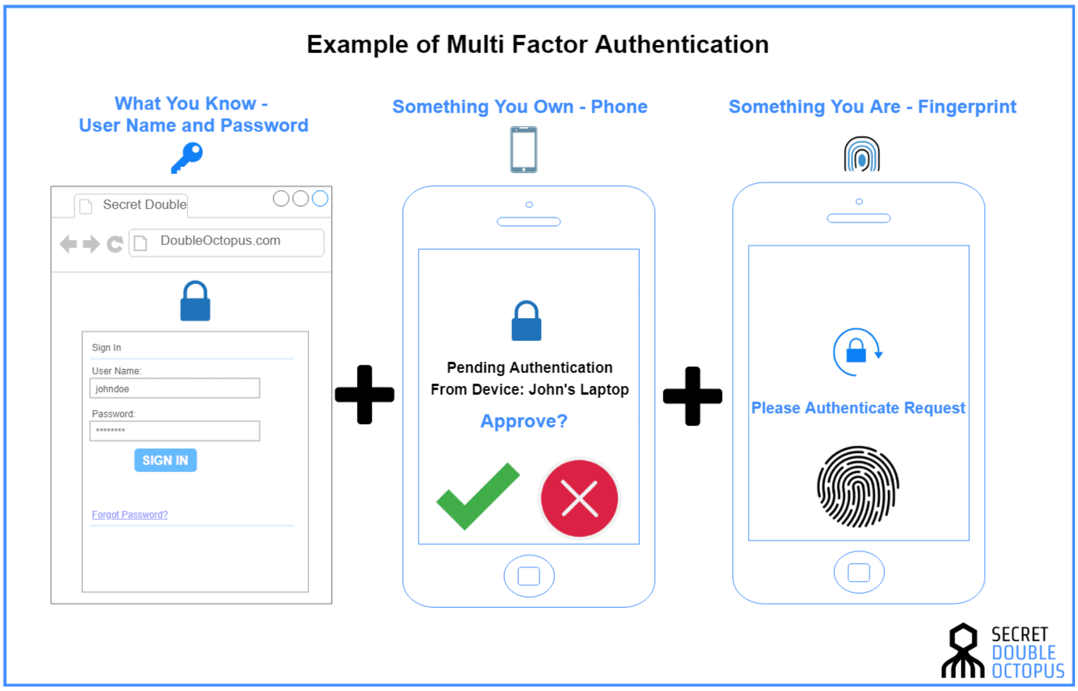


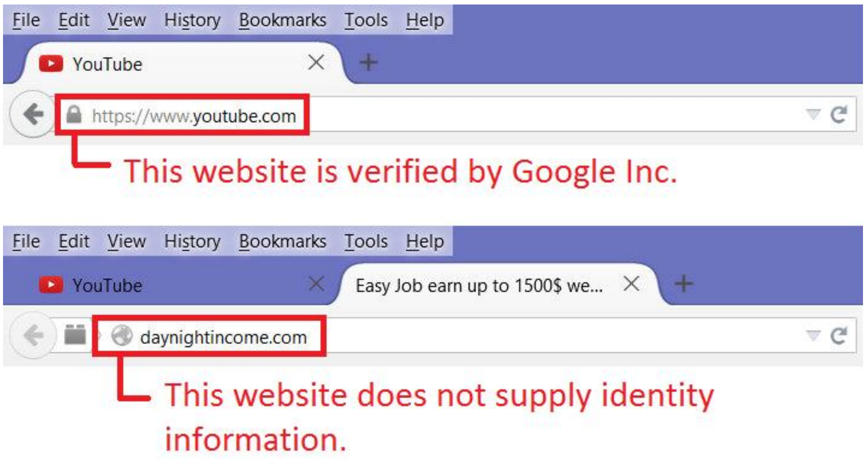
Fig. 21 Multi Factor Authentication using Smartphones

Multi-factor authentication makes an account even more secure by requiring extra information to let you log in, such as a code sent to your phone. Many large email providers and social media accounts offer this service.

- To check whether an account has multi-factor authentication, check the site's Settings page.
- This extra step might seem annoying, but it will keep your information safer than just a password alone.

5. Avoid clicking on sites that look fake or scammy.

If you're even somewhat familiar with the Internet, chances are you can recognize bad links when you see them: bad grammar, popups, "click bait" headlines, or a false-looking web address.
Avoid clicking on these sites and never download anything from them. Spending time on these kinds of websites can give your computer a virus or make it crash.


File Edit View History Bookmarks Tools Help
YouTube
https://www.youtube.com
File Edit View History Bookmarks Tools Help
YouTube
Easy Job earn up to 1500$ we...
daynightincome.com

This website is verified by Google Inc.

This website does not supply identity information.

Fig. 22 HTTPS (or Hyper Text Transfer Protocol Secure) means all communications between your browser and the website are encrypted

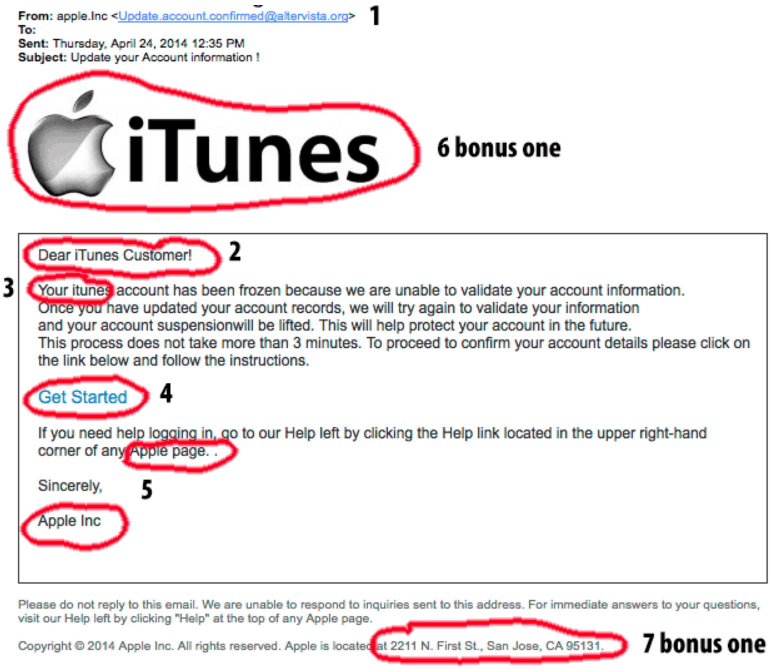
Here is a list of the most popular online scams you need to avoid in 2018:

- Phishing Email Scams
- Greeting Card Scams
- Bank Loan or Credit Card Scams
- Lottery Scams
- Hitman Scams
- Romance Scams
- Fake Antivirus Scams
- Make Fast Money Scams
- Travel Scams
- Bitcoin Scams

- Fake News Scams
- Fake Shopping Websites
- Job Offer Scams
- Tech Support Scams
- SMS Scamming

Phishing Scams

These are made based on communication via email or social networks. Scammers create a sense of urgency for victims to respond immediately to the scam emails. They'll tell you a frightening story of how your bank account is under threat and how you really need to access as soon as possible a site where you must insert your credentials in order to confirm your identity or your account.



From: apple.Inc <Update.account.confirmed@altervista.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information !

Dear iTunes Customer!

Your itunes account has been frozen because we are unable to validate your account information.
Once you have updated your account records, we will try again to validate your information
and your account suspensionwill be lifted. This will help protect your account in the future.
This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

If you need help logging in, go to our Help left by clicking the Help link located in the upper right-hand corner of any Apple page. .

Sincerely,

Apple Inc

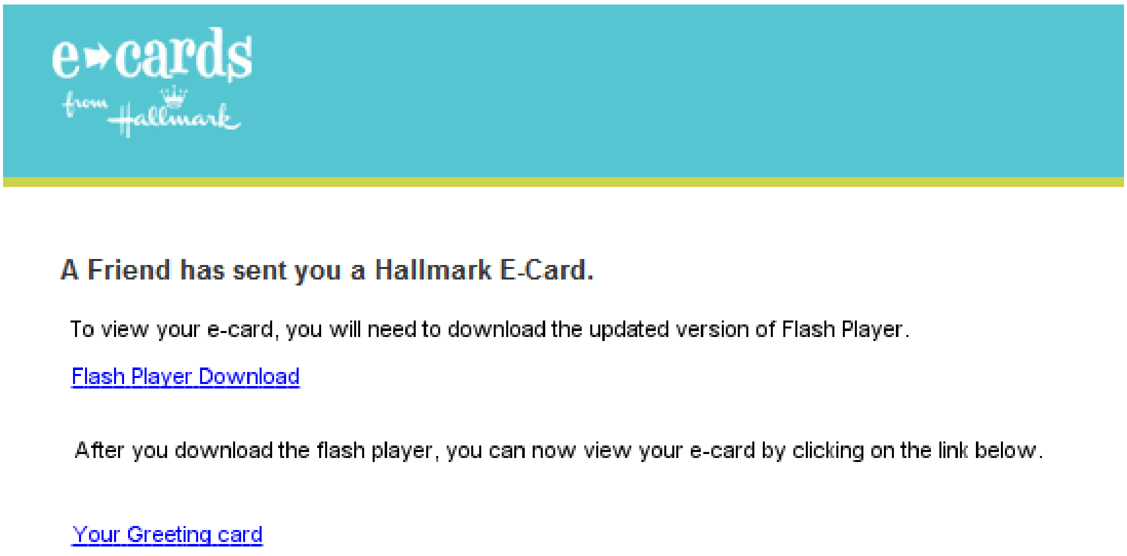
Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

Fig. 23 This is a fake email from iTunes which is not legitimate. (They are designed to look similar to original emails making it difficult for users to differentiate between the two.)

Greeting Card Scams

Greeting card scams are another old Internet scams used by malicious actors to inject malware and harvest users' most valuable data. If you open such an email and click on the card, you usually end up with malicious software that is being downloaded and installed on your operating system. Private data could be sent to fraudulent servers operated by IT criminals.



A Friend has sent you a Hallmark E-Card.

To view your e-card, you will need to download the updated version of Flash Player.

Flash Player Download

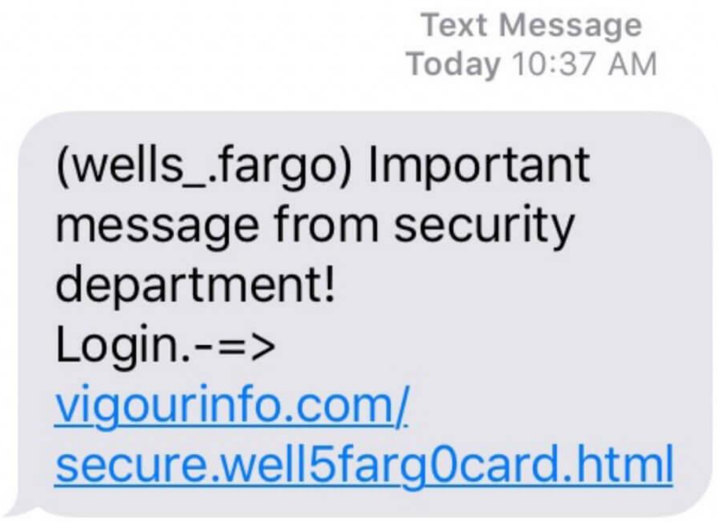
After you download the flash player, you can now view your e-card by clicking on the link below.

Your Greeting card

Fig. 24 These links could contain some malicious software/virus that would affect your computer

SMS Scams (Smshing)

Smishing (using SMS text messages) is a similar technique to phishing, but, instead of sending emails, malicious hackers send text messages to their potential victims. Be careful about these SMS you receive and don't click on suspicious links that could redirect to malicious sites trying to steal your valuable data.


Text Message
Today 10:37 AM

(wells_.fargo) Important message from security department!
Login.-=>
vigourinfo.com/secure.well5farg0card.html

Fig. 25 Thousands of such malicious URLs are sent daily to the users of smartphones

As an Android user, you'll be happy to know that malicious URLs are often easy to spot. Here are the top 3 ways to recognize a phishing attempt.

1. You don't recognize the sender:

Remember how your parents said never to talk to strangers? Well, you shouldn't be opening their URLs either. If you get a message from someone you don't know, opening the link they send you is a very poor idea. Additionally, hackers often pretend to be a reputable institution, like your bank, school, or employer, so be very careful.

2. The text message seems too good to be true:

If the SMS says you've won the lottery or a contest you didn't enter, then unfortunately for you, it's probably a hacking attempt. While it'd be lovely to become an instant millionaire, you're more likely to end up being someone with a hacked phone. So, don't open that tempting URL.

3. The link appears to be shortened or contains odd characters:

Phishing links often look a little strange. Hackers like using shortening services to create a compact URL. This trick is excellent for masking insidious URLs. But you can safely expand these links by using online tools, such as 'CheckShortURL' and 'Unfurlr'.

On the flip side, a malicious link can also be very long and contain unusual characters. Symbols like "%" are often a warning sign that the original URL is encoded and hiding its dangerous origins. When it comes to detecting malicious text messages on your Android there is a secondary way to safeguard your phone. Clicking on a link in a text message is a quick and easy way for a hacker to take control of your phone.

6. Sign up for accounts on legitimate sites only.

Consider very carefully before you make an account on a website, even if it just requires giving your email address. No matter how secure your passwords are, using them on unsafe sites will put your information in danger.

Avoid sites with misspellings or bad grammar in their addresses, which could be dangerous copycats of legitimate websites. Also look out for sites that have lots of pop-ups, or numbers or gibberish in their addresses.

In Figure 26, notice how phishing sites can look exactly the same as the original websites.

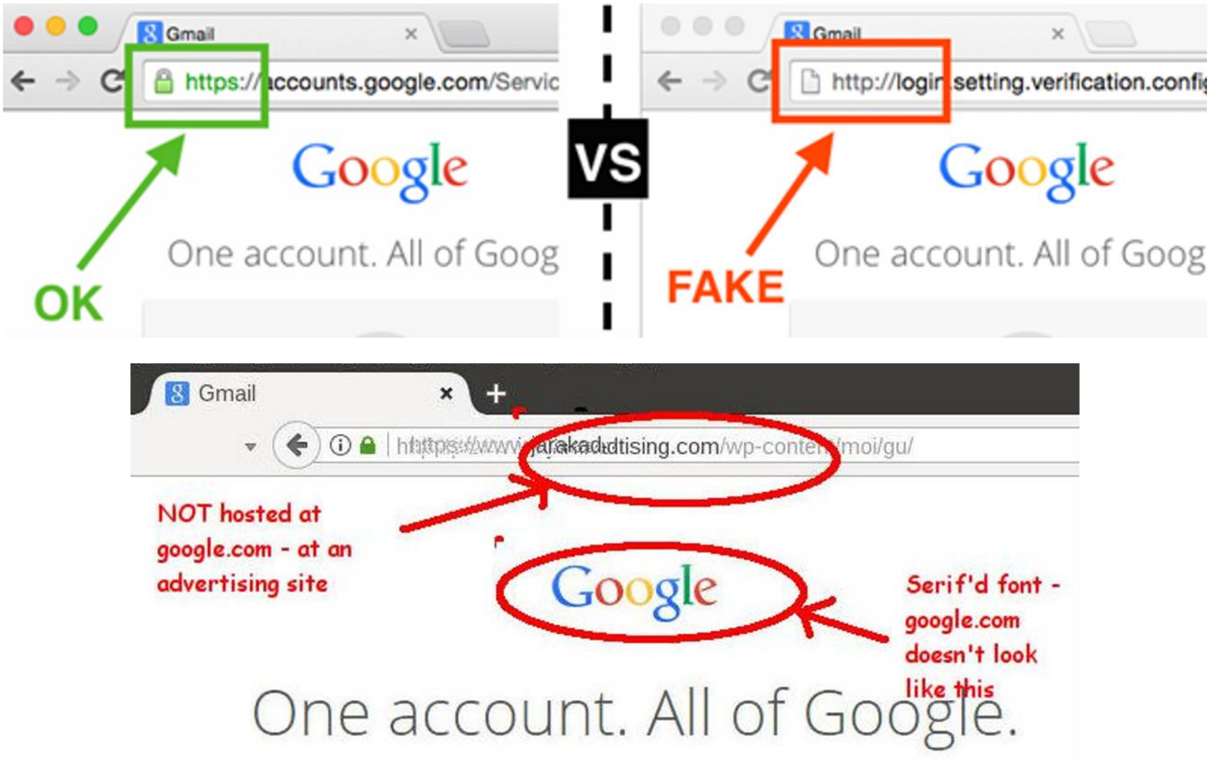

Gmail
https://accounts.google.com/Servic
Google
One account. All of Goog
OK
VS
Gmail
http://login.setting.verification.config
Google
One account. All of Goog
FAKE
Gmail
advertising.com/wp-content/moi/gu/
NOT hosted at google.com - at an advertising site
Google
Serif'd font - google.com doesn't look like this
One account. All of Google.

Fig. 26 You could land on such phishing sites even by mistyping a URL (Web Address)

7. Log out of sites when you are done using them.

Logging into a site creates a cookie in your browser, which identifies you and, if stolen, can compromise your account.

- Log out of any site you use on a public computer or network.
- Log out of any online banking or shopping site you use, even on your home computer and network.
- It’s typically OK to keep your home computer logged on to accounts like your email or social media, as long as you make sure to lock your computer if you ever step away from it.

Here’s all the data collected from you as your browse the Web:

- http://webkay.robinlinus.com/ (It is advisable to clear your browsing history/cookies often.)
- Cookies might save you the trouble of having to pick a particular city every time you visit a weather website, because the site knows what you picked last time; a cookie can also store items in your shopping basket so they’re still waiting for you when you come back days later.

- What's more, a recent study from Princeton University found that cross-site trackers embedded in 482 of the top 50,000 sites on the web were recording virtually all of their users' browser activity for analysis.
- Our internet service providers, which can now make money by selling your browsing history, letting advertisers know where you've been and what you're interested in.

8. Using Social Media and Emails safely.

- Make your profiles private
- Review what information is public on your social media profiles
- Think about whether you'll regret posting something later
- Review posts you're tagged in before approving them
- Never give personal information to someone you meet online
- Use caution when meeting in-person with someone you met online
- Use gender-neutral pseudonyms on forums
- Don't open emails or files from people you don't know

9. Use private WiFi networks, never public ones.

Public WiFi is like the kind you might find at restaurants, hotels, or airports—is often unsecured, making it easier for someone to hack into your computer. Only connect to an unsecured network if you absolutely have to, and be aware of the risks it could come with. Avoid doing online banking transactions on such networks as it is prone to hackers. If you often need WiFi on the go, try buying a Virtual Private Network (VPN), a piece of hardware that can create a secure, private connection from anywhere. Connect with care on your smartphone, too. If you can, confirm the name and login requirements of the WiFi with appropriate staff before connecting.

The problem with public Wi-Fi is that there are a tremendous number of risks that go along with these networks. While business owners may believe they're providing a valuable service to their customers, chances are the security on these networks is lax or nonexistent.

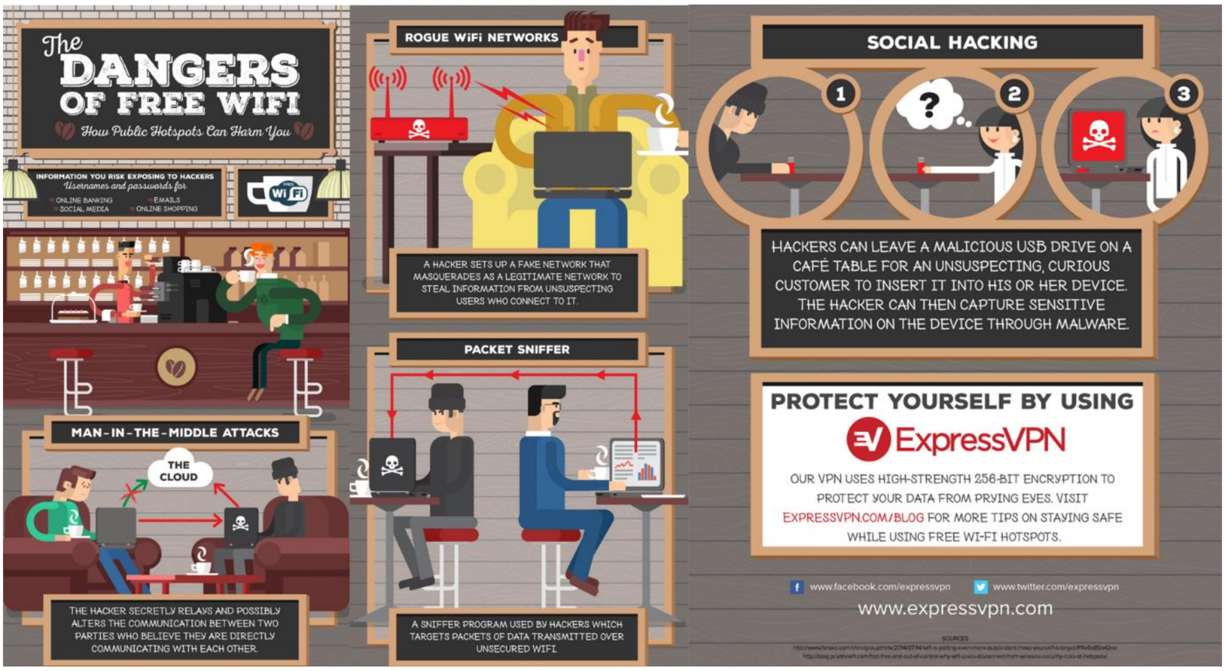

The DANGERS OF FREE WIFI
How Public Hotspots Can Harm You
INFORMATION YOU RISK EXPOSING TO HACKERS
Usernames and passwords for
ONLINE BANKING
EMAILS
SOCIAL MEDIA
ONLINE SHOPPING
FREE Wi Fi
ROGUE WiFi NETWORKS
A HACKER SETS UP A FAKE NETWORK THAT MASQUERADES AS A LEGITIMATE NETWORK TO STEAL INFORMATION FROM UNSUSPECTING USERS WHO CONNECT TO IT.
PACKET SNIFFER
A SNIFFER PROGRAM USED BY HACKERS WHICH TARGETS PACKETS OF DATA TRANSMITTED OVER UNSECURED WIFI.
MAN-IN-THE-MIDDLE ATTACKS
THE CLOUD
THE HACKER SECRETLY RELAYS AND POSSIBLY ALTERS THE COMMUNICATION BETWEEN TWO PARTIES WHO BELIEVE THEY ARE DIRECTLY COMMUNICATING WITH EACH OTHER.
SOCIAL HACKING
1
?
2
3
HACKERS CAN LEAVE A MALICIOUS USB DRIVE ON A CAFÉ TABLE FOR AN UNSUSPECTING, CURIOUS CUSTOMER TO INSERT IT INTO HIS OR HER DEVICE. THE HACKER CAN THEN CAPTURE SENSITIVE INFORMATION ON THE DEVICE THROUGH MALWARE.
PROTECT YOURSELF BY USING
ExpressVPN
OUR VPN USES HIGH-STRENGTH 256-BIT ENCRYPTION TO PROTECT YOUR DATA FROM PRYING EYES. VISIT EXPRESSVPN.COM/BLOG FOR MORE TIPS ON STAYING SAFE WHILE USING FREE WI-FI HOTSPOTS.
www.facebook.com/expressvpn
www.twitter.com/expressvpn
www.expressvpn.com
SOURCES

Fig. 26 The Dangers of Free WiFi (By ExpressVPN)

Man-in-the-Middle attacks

One of the most common threats on these networks is called a Man-in-the-Middle (MitM) attack. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and "read" them. So what you thought was private no longer is.

Unencrypted Networks

Encryption means that the information that is sent between your computer and the wireless router are in the form of a "secret code," so that it cannot be read by anyone who doesn't have the key to decipher the code. Most routers are shipped from the factory with encryption turned off by default, and it must be turned on when the network is set up. If an IT professional sets up the network, then chances are good that encryption has been enabled. However, there is no surefire way to tell if this has happened.

Malware Distribution

Thanks to software vulnerabilities, there are also ways that attackers can slip malware onto your computer without you even knowing. A software vulnerability is a security hole or weakness found in an operating system or software program. Hackers can exploit this weakness by writing code to target a specific vulnerability, and then inject the malware onto your device.

Snooping and Sniffing

Wi-Fi snooping and sniffing is what it sounds like. Cybercriminals can buy special software kits and even devices to help assist them with eavesdropping on Wi-Fi signals. This technique can allow the attackers to access everything that you are doing online — from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even hijack your accounts.

Malicious Hotspots

These “rogue access points” trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Say you’re staying at the Goodnyght Inn and want to connect to the hotel’s Wi-Fi. You may think you’re selecting the correct one when you click on “GoodNyte Inn,” but you haven’t. Instead, you’ve just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information.

How to stay safe on public Wi-Fi?

The best way to know your information is safe while using public Wi-Fi is to use a virtual private network (VPN), like Norton WiFi Privacy, when surfing on your PC, Mac, smartphone or tablet. However, if you must use public Wi-Fi, follow these tips to protect your information.

Don’t:

Allow your Wi-Fi to auto-connect to networks

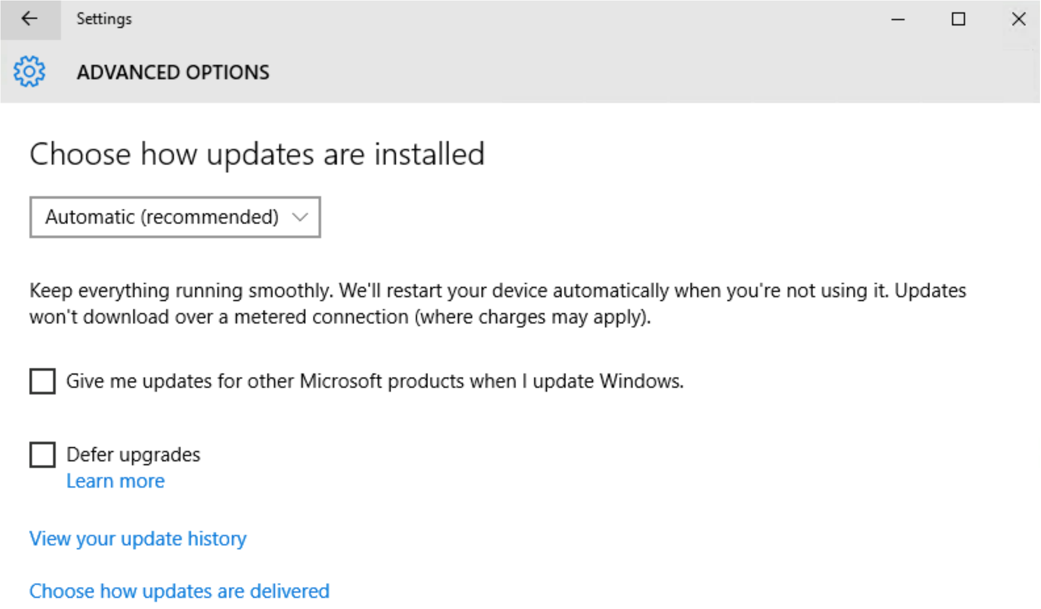
- Log into any account via an app that contains sensitive information. Go to the website instead and verify it uses HTTPS before logging in
- Leave your Wi-Fi or Bluetooth on if you are not using them
- Access websites that hold your sensitive information, such as such as financial or healthcare accounts
- Log onto a network that isn’t password protected

Do:

- Disable file sharing
- Only visit sites using HTTPS
- Log out of accounts when done using them
- Use a VPN, like Norton WiFi Privacy, to make sure your public Wi-Fi connections are made private

10. Keep your computer's software up to date.

- Most software updates come with security upgrades, so it's important that you have the latest version at all times.
- Upgrading software allows your computer to benefits from additional protections. Ensuring your system has the latest defensive solutions help limit the threat posed by malware and hackers.
- Malicious parties are continually innovating, devising new ways of attacking users' systems, and in response, the IT security industry has to find ways of reducing or eliminating this threat.
- However, end users can only benefit from the latest security tools and if they keep their software up to date. To easily download updates as soon as they come out, turn on automatic updates in your computer's settings.



Choose how updates are installed

Automatic (recommended)

Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).

☐ Give me updates for other Microsoft products when I update Windows.

☐ Defer upgrades
Learn more

View your update history

Choose how updates are delivered

Fig. 27 Always choose automatic updates in the Windows Update Settings

4. Conclusion

Events from 2017-18 have shown that technological advancements and their accelerated rate of adoption by end users globally, have brought a number of previously unthinkable scenarios within the realm of possibility.

Now is the time for users at every level, and ultimately, the public as a whole, to understand that cybersecurity not only depends on the providers they choose to safeguard it, but also on themselves and the fact that there is still a lot more work to be done. It is not possible to protect something without first understanding what it is, and knowing why we need to protect it.

Understanding these threats and building awareness about how to mitigate them is critical to protecting the confidentiality, integrity and availability of information of various stakeholders in our society, the same information that has become the basis for a number of activities (both lawful and otherwise).

It is hoped that the upcoming years will help shed some light, for readers, on the key problems that have to be addressed in order to make progress toward a safer future.

The summary of the key observations and inferences that were understood are provided here:

Macro environment:

1. The annual breach rate almost doubled to 88 records/sec. Organizations need to be prepared

with a holistic breach response plan taking into account operational, regulatory/legal and moral

considerations, if the unthinkable happens.

2. Breach notification laws are stringent in about 78% of the countries analyzed and more countries will follow suit. For global companies, developing a unified control framework to address breach notification laws across states will simplify the compliance process.

3. State actors are active, taking on big corporations across borders. Actively participating in local regulator or agency-led attack simulation exercises can help preparedness for D-day.

4. Security products are made by mortals. The research data indicates a propensity to have residual vulnerabilities. Test your security stack also regularly for weaknesses and keep the vendors accountable.

Micro environment:

1. Security budgets still form a meager portion of IT budget allocations despite the high visibility brought by cyber-attacks. Boards need to have expertise and knowledge of cyber risks and make informed choices to enable the IT executive leadership with necessary resources.

2. Metric tracking across preventive, detective and response controls in organizations seem to be minimal except for verticals like Banking which are more mature.

3. Industrial benchmarking seems distant and mostly based on personal relationships, where happening in pockets. Benchmarking can be enabled through sharing networks or vendor relationships.

4. Applications continue to be the soft underbelly for hackers to target. Organizations still struggle with imbibing security in the DevOps processes and this will have to be an area of focus.

5. Server-less Computing is fast catching up as a means to on board business functionality on the cloud, but the security challenges related to the same are not well understood. Organizations need to find compensatory controls while onboarding business functions into FaaS/Server-less models.

6. Organizations are just beginning to categorize IOT assets in the enterprise environments. We are expecting organizations to find the quick path to detect and address IOT threats which are not device-dependent but can work in other layers like the network or edge.

Meso environment:

1. Organizations need to move from generic TI consumption to more actionable and targeted intelligence.

2. Information sharing within the same industry remains elusive due to legal challenges. Organizations need to enable more resources towards threat hunting internally to be able to contribute back to the community.

3. Cyber insurance still has not seen mainstream adoption and organizations can explore it as a secondary risk transfer tool.

In the future, investment in security automation needs to be strategic to reduce the threat detection and response cycles. Permissioned blockchain which clearly has some utility for specific use cases related to security, identity management and compliance should be on the radar of security teams.

5. References

- Brian Krebs | Krebsonsecurity.com
- Kaspersky Labs | Threatpost.com
- Errata Security | blog.erratasec.com
- Security Bloggers Network | SBN – The Feed
- Sophos | Naked Security Blog
- Paul's Security Weekly | securityweekly.com
- The Security Ledger | securityledger.com
- CSO Online | @csoonline.com
- Dark Reading | @DarkReading.com
- PC World | Pcworldmag.com
- CNET | cnet.com
- Computerworld | computerworld.com
- KPMG | kpmg.com
- Times of India | timesofindia.com
- Privacy Rights | privacyrights.org
- Symantec | Symantec.com
- YouTube | youtube.com
- Medium | medium.com
- Cisco | cisco.com
- Deloitte | deloitte.com
- ESET | eset.com
- Ernst and Young | ey.com
- Pwc | pwc.in
- Research Gate | researchgate.net
- Academia | academia.edu

MACYS