CERT-MU eSecurity Newsletter

Featured

Virtual Currency and Its use in Cybercrime

The Dark Side of Online Gaming

Volume 7 | Issue 2| December 2017

CERT–MU

Computer Emergency Response Team of Mauritius (CERT-MU)

Your Partner in Cyber Security

www.cert-mu.org.mu

CERT-MU SERVICES

Reactive Services:

⇒ Incident Handling
⇒ Vulnerability Scanning and Penetration Testing

Proactive Services:

⇒ Dissemination of Information Security News, including virus alerts, advisories, vulnerability notes and warnings on latest cyber-attacks
⇒ Awareness campaigns on different Information Security themes for corporates, youngsters and the public in general
⇒ Organisation of international events such as Safer Internet Day and Computer Security Day
⇒ Organization of professional trainings on Information Security areas
⇒ Provision of educational materials through publications (includes guidelines, e-security newsletters, brochures, booklets, flyers) and a dedicated cyber security portal

Security Quality Management Services:

⇒ Assistance to organisations for the implementation of Information Security Management System (ISMS) based on ISO 27001
⇒ To conduct third party information security audits
⇒ To carry out technical security assessment of ICT infrastructure of organisations

Cyber Security Portal

The Cyber Security Portal is an initiative of CERT-MU to sensitise and raise awareness of the general public on technological and social issues facing Internet users .

The Portal consists of Internet best practices for:

⇒ Organisations
⇒ Parents
⇒ Kids
⇒ Home users

More information is available on:
www.cybersecurity.ncb.mu

In this Issue:

Featured

Virtual Currency and its use in Cybercrime

The Dark Side of Online Gaming

Shop Online Safely

News Section

Zeus Panda targeting holiday shoppers

19 Year Old TLS Vulnerability Weakens Modern Website Crypto

Security Tips

Guidelines and Security Tips

NEWSLETTER TEAM

Dear Readers,

Greetings from CERT-MU and welcome to the last issue of CERT-MU eSecurity Newsletter for the year 2017.

This e-Security Newsletter is aimed at providing our key readers an overview of the key developments on the information security arena.

This edition covers in depth information about Virtual Currency and its use in Cyber-crime. Virtual Currency/ Crypto Currency has been gaining much popularity since its introduction in the Digital world. Many people has started understanding the use and purpose of cryptocurrency. It is a new revolution in our technological field and a form of digital money. However, cybercriminals are finding it very attractive to conduct their illicit activities due to the benefits which it provides.

Our second article covers the dark side of online gaming. As online games are becoming more and more popular, it is very important to know about its darker sides and what precautions parents can take to prevent their children from becoming the victims of the risks associated with online gaming.

Thirdly, a third article focuses on online shopping. In this festive season, people are making more online shopping as they find it more convenient and less expensive. Nevertheless, cybercriminals are always watching and tricking people to carry out their malicious activities. Thus, some useful tips are highlighted in this article.

Other issues highlighted in this e-security newsletter include latest information security news, CERT-MU events and security tips and guidelines.

We hope that you will find the articles interesting and enjoy reading!

CERT-MU wishes you all a Merry Christmas and a Safe Happy New Year 2018.

Virtual Currency and Its Use in Cybercrime

Information technology and the spread of the Internet have revolutionized the financial system. The emergence of new technologies has brought many innovations and one of them is virtual currencies. Virtual currency, also known as virtual money is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. Virtual currency has been promoted as a great utility for consumers and gained popularity during the past few years. People can now save, transfer and exchange money with more ease, at greater speed, and with fewer costs. Mobile technologies are now allowing people to make small-value electronic payments from their mobile phones. While these technologies offer ample benefits, they also have their dark sides. Virtual currency is known for its use in terrorism and other cyber-criminal activities. Since they are not tied to traditional currencies, can be managed through the Internet and due to its anonymity, cybercriminals find virtual currency an attractive target to conduct illicit activities.

Common Virtual Currencies

Litecoin (LTC)

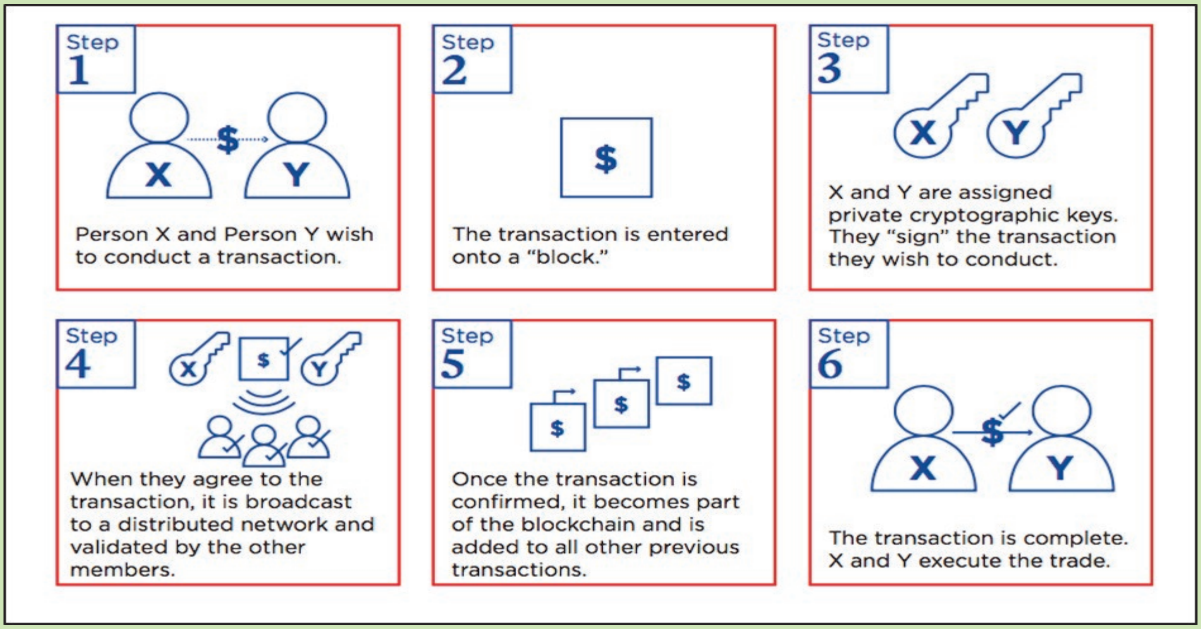
Litecoin, launched in the year 2011, was among the initial cryptocurrencies following bitcoin and was often referred to as ‘silver to Bitcoin’s gold.’ It was created by Charlie Lee, a MIT graduate and former Google engineer. Litecoin is based on an open source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer grade. Although Litecoin is like Bitcoin in many ways, it has a faster block generation rate and hence offers a faster transaction confirmation. Other than developers, there are a growing number of merchants who accept Litecoin.

Bitcoin (BTC)
Bitcoin is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency, as the system works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly through the use of cryptography, without an intermediary. These transactions are verified by network nodes and recorded in an immutable public distributed ledger called a blockchain. Bitcoin was invented by an unknown person or group of people under the name Satoshi Nakamot and released as open-source software in 2009.

What is Blockchain?
A blockchain is a type of distributed ledger, a copy of which is stored on each instance of a distributed system. Each new entry (known as a block) is certified through the creation of a unique fingerprint that incorporates the previous block, forming a "chain" and cryptographically creating an indelible record of previous transactions. All copies of the blockchain are updated with changes that take place. In the case of Bitcoin, the blockchain is public, records transactions, and enables the cryptocurrency to be decentralized.

The blockchain's appeal as a secure, decentralized database has provoked speculation about its potential for applications across a range of fields. Blockchains can potentially be used to streamline financial transactions; track the origins and legitimacy of precious gems; improve the insurance industry; create secure patient records across healthcare systems; maintain accurate international customs, shipping, and distribution records; secure voting; and help protect property in unstable markets by creating a more stable non-state ownership record network.

But potential obstacles remain to the blockchain's expansion due to its indelibility and irreversibility. Human error, hacks, and laws governing consumer rights to data deletion or correction pose challenges for the broad adoption of the blockchain. For example, after fraudulent Bitcoin transactions lost customers tens of millions of dollars in August 2016, the blockchain's irreversibility hindered the amelioration of the breach. And in most of the blockchain's potential applications, the database would only be viewable by a select audience, unlike the public Bitcoin blockchain.


Step 1
X
$
Y
Person X and Person Y wish to conduct a transaction.
Step 2
$
The transaction is entered onto a "block."
Step 3
X
Y
X and Y are assigned private cryptographic keys. They "sign" the transaction they wish to conduct.
Step 4
X
$
Y
When they agree to the transaction, it is broadcast to a distributed network and validated by the other members.
Step 5
$
$
$
Once the transaction is confirmed, it becomes part of the blockchain and is added to all other previous transactions.
Step 6
X
$
Y
The transaction is complete. X and Y execute the trade.

Zcash (ZEC)
Zcash, a decentralized and open-source cryptocurrency launched in the latter part of 2016, looks promising. "If Bitcoin is like http for money, Zcash is https," is how Zcash defines itself. Zcash offers privacy and selective transparency of transactions. Thus, like https, Zcash claims to provide extra security or privacy where all transactions are recorded and published on a blockchain, but details such as the sender, recipient, and amount remain private. Zcash offers its users the choice of 'shielded' transactions, which allow for content to be encrypted using advanced cryptographic technique or zero-knowledge proof construction called a zk-SNARK developed by its team.

Dash
Dash (originally known as Darkcoin) is a more secretive version of Bitcoin. Dash offers more anonymity as it works on a decentralized mastercode network that makes transactions almost untraceably. Launched in January 2014, Dash experienced an increasing fan following in a short span of time. This cryptocurrency was created and developed by Evan Duffield and can be mined using a CPU or GPU. In March 2015, 'Darkcoin' was rebranded to Dash, which stands for Digital Cash and operates under the ticker – DASH.

Ripple (XRP)

Ripple is a real-time global settlement network that offers instant, certain and low-cost international payments. Ripple enables banks to settle cross-border payments in real time, with end-to-end transparency, and at lower costs. Released in 2012, Ripple's consensus ledger -- its method of conformation – does not need mining, a feature that deviates from bitcoin and altcoins. Since Ripple's structure doesn't require mining, it reduces the usage of computing power, and minimizes network latency. Ripple believes that 'distributing value is a powerful way to incentivize certain behaviors' and thus currently plans to distribute XRP primarily "through business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP.

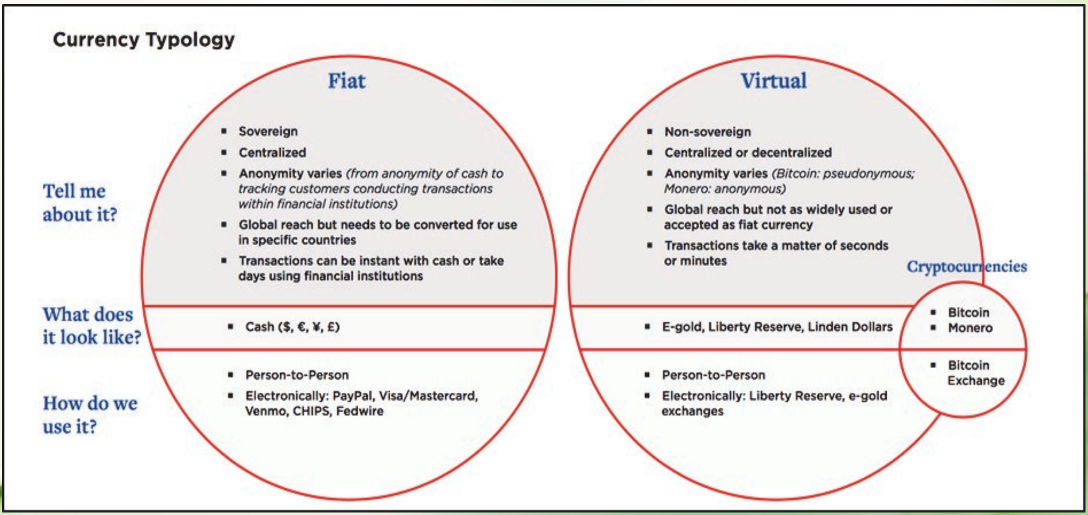
Monero (XMR)

Monero is a secure, private and untraceable currency. This open source cryptocurrency was launched in April 2014 and soon spiked great interest among the cryptography community and enthusiasts. The development of this cryptocurrency is completely donation-based and community-driven. Monero has been launched with a strong focus on decentralization and scalability, and enables complete privacy by using a special technique called 'ring signatures.' With this technique, there appears a group of cryptographic signatures including at least one real participant – but since they all appear valid, the real one cannot be isolated.

The Topology of Virtual Currency

Nowadays, there are 2 types of currencies—Fiat Currency and Virtual Currency. Fiat money is a currency without intrinsic value established as money by government regulation. The value of fiat money is derived from the relationship between supply and demand.

Virtual currencies, and especially cryptocurrencies, are at the leading edge of this financial revolution. While they vary along three main axes, virtual currencies lack sovereign backing. Firstly, these currencies can be non-convertible or convertible. Non-convertible currencies operate within a closed virtual platform. Examples include currencies used in massively multiplayer online role- playing games, where no sanctioned mechanism exists to translate the virtual unit into at currency. In these systems, however, black market exchanges may spring up, effectively offering some degree of convertibility. Convertible currencies, by contrast, have a defined equivalent value in at currency and can be exchanged, through either floating or pegged rates. Secondly, Virtual Currencies vary in their degree of anonymity. Generally, they fall between the almost total anonymity of cash exchanges and the traceability and disclosure of online payments through the traditional banking system, making them appealing to legitimate users concerned about privacy.



Currency Typology

	Fiat	Virtual	Cryptocurrencies
Tell me about it?	▪ Sovereign ▪ Centralized ▪ Anonymity varies *(from anonymity of cash to tracking customers conducting transactions within financial institutions)* ▪ Global reach but needs to be converted for use in specific countries ▪ Transactions can be instant with cash or take days using financial institutions	▪ Non-sovereign ▪ Centralized or decentralized ▪ Anonymity varies *(Bitcoin: pseudonymous; Monero: anonymous)* ▪ Global reach but not as widely used or accepted as fiat currency ▪ Transactions take a matter of seconds or minutes	
What does it look like?	▪ Cash ($, €, ¥, £)	▪ E-gold, Liberty Reserve, Linden Dollars	▪ Bitcoin ▪ Monero
How do we use it?	▪ Person-to-Person ▪ Electronically: PayPal, Visa/Mastercard, Venmo, CHIPS, Fedwire	▪ Person-to-Person ▪ Electronically: Liberty Reserve, e-gold exchanges	▪ Bitcoin Exchange

Recently, new entrants in the virtual currency space have focused on complete anonymity by developing techniques to obfuscate the true origins of Bitcoin transactions. Cybercriminals are making use of new cryptocurrencies such as Monero, which has been called the "drug dealer's cryptocurrency of choice because of its enhanced anonymity properties. In August 2016, Monero gained popularity after AlphaBay, the dark web market, started accepting it as a Bitcoin alternative. Monero attempts to ensure users' privacy by combining multiple transactions, hiding the amount of each transaction and obscuring the recipient of the funds. By January 2017, it had become 27 times more valuable due to its adoption in online criminal markets *(Source: Greenberg, "Monero, The Drug Dealer's Cryptocurrency of Choice.)* It is already drawing the attention of law enforcement for its facility of use by criminals on the dark web. Similarly, Dark Wallet, which seeks to make de-anonymizing Bitcoin transactions impossible, disrupts the blockchain's potentially identifying aspects by combining random contemporaneous transactions and then encrypting recipients' information so it does not appear on the blockchain. This method explicitly seeks to enable illicit finance.

Finally, virtual currencies may be centralized or decentralized. But, the question which raises is that how to engender trust without government or central bank backing. For centralized Virtual Currency, an administrator issues the currency, maintains a unified central payment ledger and retains the power to withdraw currency from circulation. This central institution acts as the fundamental repository and guarantor of trust. Examples include Linden Dollars, available in the Second Life virtual reality world; Perfect Money; units of the now-defunct e-gold; and LRs, units used on Liberty Reserve.

As discussed above, decentralized virtual currencies have no central administrator or oversight, and trust is based on consensus validation. They often rely on cryptography for their operations and use distributed ledger technologies to record transactions. As the most widespread decentralized virtual currency, Bitcoin has also faced the most real-world vetting. It survived a software glitch in 2013 and a security breach and bankruptcy of its largest exchange in 2014. It has found acceptance as a currency among retailers including popular websites, for example Expedia and Overstock.com.

Benefits of Virtual Currency

Cybercriminals are motivated and more likely to use virtual currencies due to certain perceived advantages, which are specifically:

- ⇒ The greatest degree of anonymity for both users and transactions
- ⇒ The ability to quickly and confidently move illicit proceeds from one country to another
- ⇒ Low volatility, which results in lower exchange risk, increasing the virtual currency's ability to be an efficient means to transmit and store wealth.
- ⇒ Widespread adoption in the criminal underground
- ⇒ Trustworthiness

Virtual currencies such as Bitcoin offer two primary advantages as compared to legacy financial technology, which are lower costs and faster transaction speeds. Lower transaction cost was identified as one of the main goal by the founder of Bitcoin – Satoshi Nakamoto when conceptualizing the virtual currency. As Nakamoto noted, requiring financial institutions to act as trusted third parties in transfers raises the overall costs. In 2015, the global average cost of sending a $200 remittance, for example, was close to 8 percent *(Source: World Bank Group, "Migration and Remittances Factbook 2016 Third Edition," (Washington, D.C.: World Bank, May 2, 2016).*

Virtual currencies allow for improved speed of transactions by adapting the method of recording the value transfers with very low latency periods. Increased transaction speeds unlock ancillary advantages as well. Faster transfers reduce settlement and credit risks involved in waiting for funds to transfer, and they enable parties to use capital more effectively. Greater speed also reduces a user's exposure to exchange rate fluctuations, a source of concern given the volatility of many early-stage VCs. The current concern over the scalability of Bitcoin highlights how important speed is to virtual currencies.

As the scale and use of these currencies has increased, the time to validate each transaction has grown as well, leading supporters to search for technical solutions and skeptics to wonder whether the inability to process a growing number of transactions at sufficient speeds will impose a ceiling to the technology.

The potential of virtual currencies to bring about benefits can be seen in the remittance market. Payphil, Sentbe, and similar Bitcoin transfer services have halved remittance costs between South Korea and the Philippines, and they account for 20 percent of the total remittance flows between the two countries. *(Source: Buenaventura "There's a $500 Billion Remittance Market")*. It is worth noting, though, that unlike direct Bitcoin transfers, many Bitcoin remittance services and exchanges are more akin to payment systems, benefiting from the ease of exchange of Virtual currencies without the risks of anonymity or pseudonymity.

Conscious of these advantages, criminal groups have embraced virtual currencies in self-contained online marketplaces such as AlphaBay, and ecosystems like Liberty Reserve, described above, and Silk Road. In these circumstances, virtual currencies are used in a number of ways, and because of their broad utility, particularly, their convertibility, criminals are more likely to adopt them.

Another reason due to which criminal groups use virtual currencies is to purchase and sell technical tools required to conduct cyberattacks such as exploits designed to take advantage of particular software vulnerabilities. Virtual currencies are also used to purchase stolen data, monetized on the dark web. Ransomware is another example of how these currencies enable cybercrime. Most importantly, they facilitate anonymous transactions or make available, for a fee, extra steps to ensure anonymity.

The Growth and Scale of New Payment Technologies

Three of the key characteristics that determine the scale that virtual currencies can reach are their degree of centralization, their liquidity and convertibility, and the network effect, whereby a service becomes more useful to all users the more people use it.

Centralisation

As virtual currencies and payment systems expand,it is likely that they will become increasingly de facto centralized, even though they began as a deliberately decentralized system. Experts have observed that online peer production projects such as Wikipedia are likely to conform to the so-called iron law of oligarchy, which holds that even organisations set up in a distributed fashion will increasingly converge around a few institutions as they grow. This is in part because as more people begin to use virtual currencies and cryptocurrencies, investments in necessary infrastructure will become less expensive as economies of scale take hold. Additionally, users will have more confidence that a transaction will go through, which will reduce volatility and make currencies more consumer-friendly.

Liquidity and Convertibility

Liquidity and convertibility are essential components for any currency, including virtual currencies, to become usable by large groups of people. A currency needs to be useful for purchasing a variety of goods or it will be challenging for that system to scale and gain promi- nence. It also needs to feature easy convertibility to fiat currency. Some liquid, highly convertible, nearly anonymous stores of value do exist and are extremely common. For example, gift cards to Amazon.com approach the liquidity of cash, are easy to obtain and therefore represent a growing money laundering threat.

Abuse of Virtual Currency by Cybercriminals: The Case of Bitcoin

Bitcoin's characteristics including its irreversibility, use of the blockchain, pseudonymity, and decentralization, make it more flexible, private, and less amenable to regulatory oversight, as per experts. It has also proven to be a useful tool for illicit financial activities. According to Europol's *The 2015 Internet Organised Crime Threat Assessment*, Bitcoin is becoming more prominent in investigations of payments between criminals and was estimated to be responsible for more than 40 percent of these payments in the European Union in 2015.

A major obstacle to Bitcoin scaling as a tool for terrorism finance is the blockchain, the publicly accessible ledger that records all transactions that take place through Bitcoin. Thus, while Bitcoin wallets are not necessarily linked to real identities (though exchanges in well-regulated jurisdictions do establish these links), it will always be possible to unravel a chain of transactions. Experts have explained that cryptocurrencies are part of the arms race of cryptography: As one person develops a cryptographic algorithm allowing transactions to be more anonymous, another person immediately begins work on solving it to peel back the anonymity. Once the sequence of transaction is revealed, Bitcoin addresses can be linked to real-life identities through forensic techniques, after which one's entire transaction history becomes visible.

Despite of this, cybercriminals have made and continue to make extensive use of Bitcoin. Bitcoin is often used in ransomware attacks, a threatening development that connects cybercrime to financial crime. Ransomware attacks is closely linked to Bitcoin because of the anonymity required to launch successful attacks, which Bitcoin readily provides. Online criminals conducting ransomware attacks deploy malware to encrypt data and demand a ransom before providing the decryption key. Recently, ransomware attacks have spiked in frequency and significance. The latest 2017 ransomware attacks which include WannaCry and the Petya made use of Bitcoin to demand for ransom from victims.

Experts have also observed that there has been a 3,500 percent increase in criminals' use of the net infrastructure that supports ransomware *(Source: Mark Ward, "'Alarming' Rise in Ransomware Tracked," BBC News, June 7, 2016)*. Similarly, Symantec's Report on Ransomware and Businesses 2016 estimates that global losses to ransomware are in the hundreds of millions of dollars. Ransomware attackers, mostly from Eastern Europe and China, target businesses and local governments; as a result, companies are stockpiling bitcoins in the event that they should be hit. Hospitals are a particular target for ransomware, because in order to function, they have an absolute and immediate need for their data, including patient records and medicine histories.

Conclusion

Virtual currencies are appealing to cybercriminals for the same reason they appeal to legitimate actors. Virtual Currencies are mainly distinguished by their global reach, often a decentralized structure, varying degrees of anonymity, rapid transactions, and minimal costs. The risk that terrorists will increasingly use virtual currencies to move and store money in the future indicates a need to consider whether our current financial regulatory architecture is up to the task of preventing this eventuality. Observers and policymakers have highlighted a need for vigilance to prevent this from occurring, which in practice translates into adaptations to financial regulation and compliance. Additionally, it means a policy posture on financial technology oversight that is designed to both protect the benefits that can be afforded by virtual currencies and prevent their abuse.

The Dark Side of Online Gaming

As the Internet permeates every aspect of the economy and society, it is also becoming an essential element of our children's lives. While it can bring considerable benefits for their education and development, it also exposes them to online risks such as access to inappropriate content, harmful interactions with other children or with adults, and exposure to aggressive online games. While online games may be entertaining, it also has its own share of risks. Children can also put their computer systems at risk and disseminate their personal data without understanding the potential long-term privacy consequences. In this article, the risks associated with online gaming will be discussed.

Online gaming involves both technological and social risks, which are described as follows:

Cyberbullying

Online gaming has become a popular activity amongst children and teenagers. Many video games – whether they are console, web, or computer-based, allow users to play with friends they know in person and others they have met only online. While gaming can have positive benefits like making new friends, socializing, and learning how to strategize and problem solve, it is also another place where cyberbullying occurs.

Anonymity of players and the use of avatars allow users to create alter-egos or fictional versions of themselves, which is part of the fun of gaming. But it also allows users to harass, bully, and sometimes gang up on other players, sending or posting negative or hurtful messages and using the game as a tool of harassment. If someone is not performing well, other children may curse or make negative remarks that turn into bullying, or they might exclude the person from playing together.

Since players are anonymous, they cannot necessarily be held accountable for their behavior, and their harassment can cause some players to leave games. Some anonymous users use the game as a means to harass strangers or to get their personal information, like user names and passwords.

There are things adults can do to prevent cyberbullying of children who are gaming:

⇒ Play the game or observe when the gaming happens to understand how it works and what a child is exposed to in the game.

⇒ Check in periodically with your child about who is online, playing the game with them.

⇒ Teach your children about safe online behavior, including not clicking on links from strangers, not sharing personal information, not participating in bullying behavior of other players, and what to do if they observe or experience bullying.

Addiction

The world of online multi-player gaming has grown increasingly popular as gamers adopt new roles and personalities in "massive multiplayer online role-playing games," or MMORPGs such as World of Warcraft, RuneScape and Everquest. These games incite kids as young as 12 to play for hours and putting all other activities aside. Consequently, this may have long term effects including aggressiveness, anti-social behaviour.

Privacy Problems

The social nature of online gaming allows cybercriminals to manipulate conversations. They may single out your child in a general chat channel and then start sending personal messages that ask for detailed personal information. By piecing together data from games and other sources, hackers may be able to establish accounts in your child's name or gain access to existing accounts.

It is therefore recommended that kids never create user names that are derivatives of their real names, or that might give away their location or age. In addition, never give away any kind of personal information and make sure user names and passwords are different across different games and gaming sites.

Personal Information Left on Consoles and PCs

Another online gaming danger comes from consoles or PCs themselves. When they have outlived their usefulness, users often forget to delete their files and personal information, in turn putting their financial and private lives at risk. You should wipe all personal data from games consoles, tablets and smartphones and then perform a factory reset. The specific tools or procedures needed might vary depending on the type of device, thus it is important to research this for each device. Also, remember that some devices might include storage areas that are not affected by the device's erase functions. If the device includes PC-compatible storage drives (e.g., SD cards), connect them to your PC and securely erase the data. For PCs, do not just rely on the "Delete" function or even formatting, since these will not actually remove data from the drive. Instead, you should use a program that removes data by overwriting the data multiple times.

Webcam Concerns

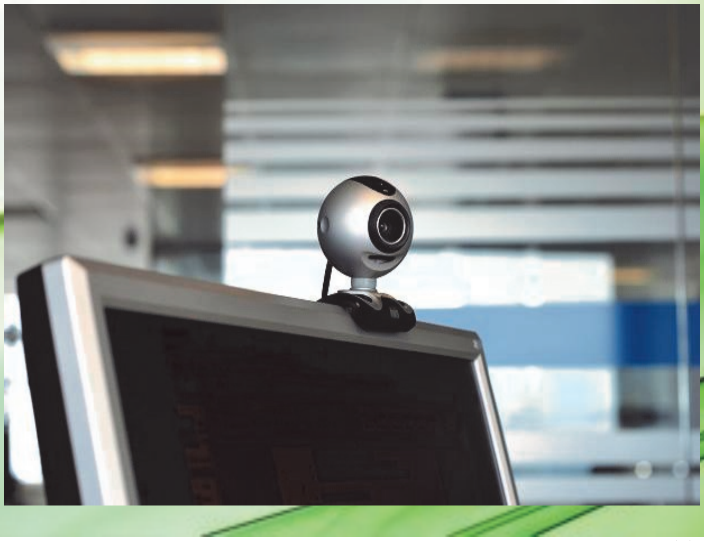
Webcams are a great piece of technology. Unfortunately, like most technological advancements, they can be twisted and abused to do things they were never meant to do. Certainly, they are great for keeping in touch with long-distance relationships, for performing online interviews, for chatting with friends, etc. But a hacked webcam becomes a spy tool that voyeurs can exploit for their own gain.

As noted by Business Insider, more than 4,500 US webcams were hacked last year and streamed onto a Russian website. Any connected device - such as a webcam or audio device - could be controlled by attackers and used to exploit your children. To help mitigate this risk, make sure to scan your system for malware regularly, and ensure that your webcam's default setting is "off".

Online Predators

Online predators are typically older gamers who use video games to lure and groom younger victims. The end result may be inappropriate messages, webcam chats or even face-to-face meetings that could lead to sexual exploitation. Online gaming gives predators the chance to build a kind of shared online experience, in effect becoming the child's defender or teammate. After defeating a tough boss or exploring a new area in game, predators form a bond with younger gamers and build a set of common experiences that lead to more personal questions. In many cases, predators seek to turn kids against their parents and by taking up the mantle of the "only person who really understands them".

Parents should therefore talk to their children about online risks, and monitoring their gameplay closely to combat this problem.



Hidden Fees

Some online games use the "freemium" model, which means they give you some content for free, however they require you to pay to access other portions of the game. For example, Windows 10 users have to pay to play certain modes of classic games without being interrupted by ads. Or a player might use real money to buy a virtual sword or piece of armor, or rack up credit card charges to gain gold or experience for his or her characters. In most cases, these games require a credit card to sign up and start playing, and it is automatically charged if users decide to purchase new items or services.

As a precaution, parents should never give out their card number for any freemium games. Even if your child is playing more traditional subscription-based games, it is a good idea to regularly check your credit card bills to make sure you are not being charged for purchases you did not agree to make. If you allow your children to use your smartphone or tablet, you should seriously consider switching off in-app updates, to prevent your children from racking up huge bills for in-app purchases without even realizing it.

Malware

Trojans may modify a legitimate app and upload the malicious version to Google Play or another legitimate marketplace. When malicious game apps are downloaded, the Trojan would execute and was capable of taking control of a user's Android device and making it part of a larger "botnet". The malware operates on a delay timer, so victims will not suspect their online game as the source.

The lesson here is to always be careful which apps you are downloading. Apps can seem legitimate, or masquerade as legitimate apps.

It is thus important to read reviews, research the developers and make sure any app is safe before downloading it onto your smartphone. And you should only download apps from reputable sources.

Make sure you're the one approving all mobile downloads, and take the time to install a reputable mobile anti-malware scanner so you can regularly check all devices in your home. Playing online isn't all fun and games—children are at risk from bullying, identity theft, credit card fraud and even sexual exploitation. Make sure to talk to your children about these risks.

The Suicidal Online Gaming: The Blue Whale Challenge

A very dangerous online game known as the Blue Whale game or Blue Whale Challenge made its apparition on the Internet this year and was targeting teenagers. Several suicide cases associated with the game were registered across the world including countries such as India, Russia, Uk, etc..

What was more alarming was that the Blue Whale game was not a downloadable game, application or software. It originated from secretive groups on social media networks. The challenge allegedly started in secret groups on the Russian social media networks and propagated on other social media networks.

The Blue Whale Challenge is believed to be a suicide game wherein a group of administrators or a certain curator gives a participant a task to complete daily, for a period of 50 days. Every day a particular task is assigned to the participant and lastly, that is on the 50th day, the final task urges the participant to commit suicide by jumping a high building. Participants were also expected to share photos of the challenges or tasks completed by them.

These daily tasks started off easy such as listening to certain genres of music, waking up at odd hours, watching a horror movie, among others, and then slowly escalated to carving out shapes on one's skin, self-mutilation and eventually suicide.

CERT-MU wishes to draw the attention of parents and teachers on this dangerous online game and request them to be vigilant and to keep an eye on what their children are sharing on their social media accounts as this game can lead to severe consequences.

Shop Online Safely

The Internet made shopping a more pleasant, cost-effective and friendly experience. It also saves considerable time and effort. However, there are associated risks with online shopping. For example, from whom, and how you pay for your purchases.

Below there are useful online shopping tips to help you to enjoy the Internet and avoid becoming the prey of cybercriminals and online scams:

Stick with trusted brands that have a strong reputation
Sticking with popular brands is as good as any advice when shopping online. Not only do you know what you're getting by way of quality and price, but you also feel more confident that these well-established names have in place robust security measures.

Look out for https URL and the padlock symbol
https, which was developed by Netscape, is an online safety protocol that encrypts information so that data can be kept private and protected. In most cases, the text in the URL is preceded by a padlock symbol (if this is missing, the website should be treated with caution).

The 's' in https incidentally, stands for secure. Websites that use https are safe because they utilise SSL (Secure Sockets Layer) to encrypt any information that is distributed online, such as your credit card details.

Search the Internet safely
Even though search engines are very useful when you are looking for products, reviews or price comparisons, you run the risk of unintentionally clicking on 'poisoned' search results that could lead you to malware instead of your intended destination. These poisoned search results are created by cybercriminals that use search engine optimisation (SEO) tricks — sometimes referred to as Black SEO — to manipulate search engine results to include malicious links. Tools such as Kaspersky's URL Advisor — or third-party browser add-ons, such as Web of Trust — can help prevent you from clicking on poisoned links and entering malicious websites.

Type the URL into the address bar
Instead of just clicking a link to take you to your chosen retailer's website, it's safer to type the retailer's URL into the address bar on your web browser. It may take a little more effort, but this simple action can help to prevent you visiting a fake or malicious website.

Manage and protect your online passwords
Using a password manager can help you to deal with multiple accounts and passwords — and to encrypt passwords that would otherwise be in plain text. Some antivirus and Internet security software products include password management and password security features.

Beware of using public Wi-Fi
When you are in a shopping mall and about to make a purchase, it can be useful to make a last minute comparison with the best deals that Internet retailers are offering. However, there can be security risks if you access the Internet via a public Wi-Fi network. Cybercriminals can intercept your data and capture your passwords, login details and financial information. If you need to access the Internet when you are out shopping, it's safer to do so via your mobile phone network.

Zeus Panda targeting holiday shoppers

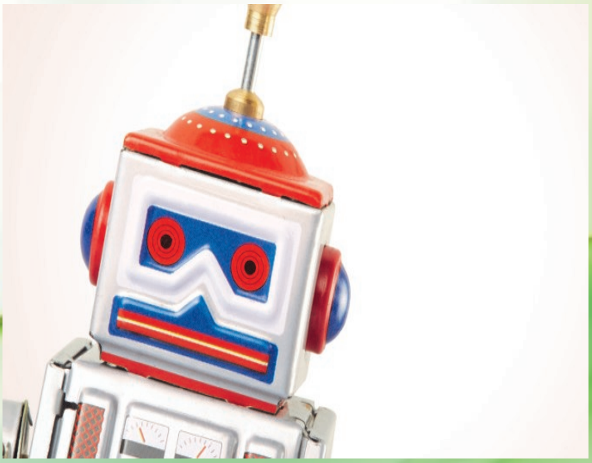
With just a few more shopping days available before the New Year, cybercriminals are taking advantage of online shoppers' buying habits by injecting the Zeus Panda banking Trojan into a wide range of retail and travel sites, along with spreading the malware through malspam.

Security firm Proof point reported that attackers are spreading Zeus Panda, which is normally a banking Trojan, to non-banking targets such as consumer and e-commerce sites to take advantage of their higher-than-usual credit card use and traffic during the holiday period. Zeus Panda is a useful criminal tool to attack users of non-banking sites because it can be configured to steal credit card numbers, addresses, phone numbers, birth date, Social Security numbers, and security question-related information such as mother's maiden name.

So far, UK and Canadian firms have headed up the target list, with cybercriminals either using an email with a malicious attachment to drop Zeus Panda, or using malicious ads that have been inserted into compromised websites. The malware then waits until the user visits an online store or bank and quietly steals the person's payment information.

Users are therefore advised to be cautious when shopping online during this festive season.

19 Year Old TLS Vulnerability Weakens Modern Website Crypto



A vulnerability called ROBOT, first identified in 1998, has resurfaced. Impacted are leading websites ranging from Facebook to Paypal, which are vulnerable to attackers that could decrypt encrypted data and sign communications using the sites' own private encryption key. The vulnerability is found in the transport layer security protocol used for Web encryption. A successful attack could allow an attacker to passively record traffic and later decrypt it or open the door for a man-in-the-middle attack, according to researchers.

ROBOT, which stands for Return Of Bleichenbacher's Oracle Threat, was named after Daniel Bleichenbacher, the researcher who originally discovered it almost two decades ago. The version of ROBOT discovered recently was through Facebook's bug bounty program, which paid an undisclosed reward to researchers Hanno Böck, Juraj Somorovsky and Craig Young who published their findings.

The vulnerability is tied to the TLS protocol and a flaw in the algorithm that handles RSA encryption keys. The attack involves using specially crafted queries designed to generate errors on TLS servers that use RSA encryption to protect communications between a user's browser and a website. The attack involves sending crafted queries that generate "yes" or "no" answers in a type of brute-force guessing attack. Using this technique, called an adaptive chosen-ciphertext attack, over time can force the TLS server to reveal the session key. That allows an attacker to then decrypt HTTPS traffic sent between the TLS server and the user's browser.

CERT-MU Event: Technical Colloquium 2017

National Computer Board
Computer Emergency Response Team of Mauritius (CERT-MU)
YOUR PARTNER IN INFORMATION SECURITY
Email: contact@cert.ncb.mu
Toll free number: 8002378
RSA
THE MOMENT YOU LINK BUSINESS RISK TO A SECURITY INCIDENT
THAT'S BUSINESS-DRIVEN SECURITY™

National Computer Board
Computer Emergency Response Team of Mauritius
FORUM OF INCIDENT RESPONSE SECURITY TEAMS (FIRST) - TECHNICAL COLLOQUIUM

The Computer Emergency Response Team of Mauritius (CERT-MU), a division of the National Computer Board (NCB) operating under the aegis of the Ministry of Technology, Communication & Innovation organised a Technical Colloquium (TC) in Mauritius from 30th November – 1st December 2017 with the theme "Emerging Threats of the Cyberspace and its Countermeasures", in collaboration with the Forum of Incident Response and Security Teams (FIRST), USA. This event was organised to commemorate the Computer Security Day 2017.

Forum of Incident Response and Security Teams (FIRST)

FIRST is a global non-profit organization based in Morrisville North Carolina, United States of America and is a recognized leader in Incident Response. It regroups 365 security teams from 78 countries including Mauritius. Through its Global Cyber security initiative, it is helping its members to share information about vulnerabilities, incidents, tools and all other issues that affect the handling of cyber security incidents. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organisations with a view to fostering cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among its members and the community at large.

The main objectives of the TC were to:

- ⇒ build capacity and improve the incident response capabilities; and
- ⇒ gauge and improve the preparedness in the identification, response, prevention and resolution of computer incidents within organisations.

The TC was expected to bring together participants from different countries. Local experts also took part in the TC. The target audience included Information Security Consultants/Analysts, Information Security Specialists, IT Managers, IT Executives, Network Engineers, System Administrators and Database Administrators etc.

The event was planned over a period of two days, comprising a full-day workshop on 30th November 2017 and one day training programme on 1st December 2017. During the workshop, the following themes were covered:

- ⇒ Mapping the Ransomware Landscape;
- ⇒ Digital Forensics;
- ⇒ Demystifying the Darknet;
- ⇒ Virtual Currency and Cybercrime;
- ⇒ Botnets – A Game changer in Cybersecurity Priorities
- ⇒ Blockchain
- ⇒ Data Loss Prevention

FIRST experts also shared their experiences during the one day training programme which was organised on the following themes:

- ⇒ Fusion Course
- ⇒ Mastering CVSSv3

There was also an exhibition to showcase the latest security products and services on 30th November 2017 by Secure Services Mauritius Ltd (SSML), TYLERS, Elysiumsecurity and ORACLE.

Guidelines and Security Tips

Guidelines

CERT-MU publishes information security guidelines on a regular basis to help and guide users in adopting best practices and implement them whenever possible. The latest guidelines published are as follows:

⇒ Guideline for Parents on Mobile Apps
⇒ Guideline on Devising a Personal Back Up Plan
⇒ Guideline on Email Encryption and Signatures
⇒ Guideline on Cyber Threat Intelligence

The guidelines can be downloaded from CERT-MU website:
www.cert-mu.org.mu

Security Tip: Holiday Traveling with Personal Internet-Enabled Devices

The Internet is at our fingertips with the widespread use of Internet-enabled devices such as smart phones and tablets. When traveling and shopping anytime, and especially during the holidays, consider the wireless network you are using when you complete transactions on your device.

The tips below are helpful to consider when traveling with Personal Internet Enabled Devices:

Know the risks
Your smart phone, tablet, or other device is a full-fledged computer. It is susceptible to risks inherent in online transactions. When shopping, banking, or sharing personal information online, take the same precautions with your smart phone or other device. The mobile nature of these devices means that you should also take precautions for the physical security of your device and consider the way you are accessing the Internet.

Do not use public Wi-Fi networks

Avoid using open Wi-Fi networks to conduct personal business, bank, or shop online. Open Wi-Fi networks at places such as airports, coffee shops, and other public locations present an opportunity for attackers to intercept sensitive information that you would provide to complete an online transaction. If you simply must check your bank balance or make an online purchase while you are traveling, turn off your device's Wi-Fi connection and use your mobile device's cellular data Internet connection instead of making the transaction over an unsecure Wi-Fi network.

Turn off Bluetooth when not in use

Bluetooth-enabled accessories can be helpful, such as earpieces for hands-free talking and external keyboards for ease of typing. When these devices are not in use, turn off the Bluetooth setting on your phone. Cyber criminals have the capability to pair with your phone's open Bluetooth connection when you are not using it and steal personal information.

Be cautious when charging

Avoid connecting your mobile device to any computer or charging station that you do not control, such as a charging station at an airport terminal or a shared computer at a library. Connecting a mobile device to a computer using a USB cable can allow software running on that computer to interact with the phone in ways that a user may not anticipate. As a result, a malicious computer could gain access to your sensitive data or install new software.

CERT-MU

Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting
Hotline: 800 2378
Email: incident@cert.ncb.mu

Vulnerability Reporting
Email: vulnerability@cert.ncb.mu

For Queries
Email: contact@cert.ncb.mu

Subscription to Mailing Lists
Email: subscribe@cert.ncb.mu