Security of Electronic-wallets

An Electronic-wallet(e-wallet) is an electronic application that enables online e-commerce transactions like purchasing goods, paying utility bills, transferring money, booking flight etc. with a financial instrument (such as a credit card or a digital currency) using smart phones or computers. A plethora of these e-wallets are provided online for downloading through "apps" to support both point of sale transactions and peer-to-peer transactions between individuals. Being preloaded with currency by the user, they are designed to be convenient to them over the traditional-wallets, by providing better manageability over their payments, accounts, receiving of offers, alerts from merchants, storing digital receipts and warranty information and being secure by requiring to access only through correct passphrase, password and such authentication information.

A number of IT companies, Banks, Telecoms firms, online e-commerce portal, taxi-services, supermarket chains etc. provide e-wallets .
A number of personally identifiable information (PII's) of the customer like his name, mobile phone number and his protected personal information like Customer card numbers, secret PIN, net banking credentials etc is permanently stored in e-wallets, requiring just final authorization from the user through means like biometrics authentication, one-time passwords(OTP) etc. The payment process involves security mechanisms like certificate pinning and use of encryption.

Threats to E-Wallets and countermeasures

Impersonation, SIM swapping

SIM SWAP Impersonation occurs when a fraudster steals information and then poses as a genuine user to do a transaction using the stolen e-wallet details and password.
SIM swaps occurs when fraudsters first collect the user's information, and use it to get his mobile phone SIM card blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudster who then generates one-time passwords using stolen information.

For prevention against Impersonation and SIM swapping attacks:

- Avoid falling prey to social engineering tricks: Financial service providers and support staff will never ask their customers for sharing their private information such as passwords or payment account numbers over email requests or phone inquiries etc.

- Some Mobile network operators send an SMS to alert their customers of a SIM swap, the affected customer can act and stop this fraud in its tracks by contacting the mobile operator immediately.

Man-in-the-middle attack and Phishing

Sophisticated threats like Man-in-the-Browser or Man-in-the-Middle attacks intercept online transactions by reading payment data from the Internet browser while the user is typing his credit card or bank account details. Phishing attacks are used to steal users' login details and personal data, making e-wallet accounts susceptible to fraud.

For prevention against phishing attacks:

The URL of the web-page should be verified, by establishing the authenticity of the website by validating its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of the browser window. Emails or text messages asking the user to confirm or provide personal information (Debit/Credit/ATM pin, CVV, expiry date, passwords, etc.) should be ignored.

Malware Attacks:

Malware attacks on apps have threatened the safety of user’s money. An attacker can inject a malware to attack the app and collect details from his phone to misuse it.

For prevention against Malware attacks:

Keep the wallet software up to date: Using the latest version of software allows receiving important stability and security fixes timely. Updates can prevent problems of various severities, include new useful features and help keep the wallet safe. Installing updates for all other software on the computer or mobile is also significant to keep the wallet environment safer.
Use security software: Applications for detecting and removing threats, including firewalls, virus and malware detection and intrusion-detection systems, mobile security solutions should be installed and activated.

Best Practices for Users to remain safe:

- **Enable Passwords On Devices**: Strong passwords should be enabled on the user's phones, tablets, and other devices before e-wallets can be used. Additional layers of security provided by these devices should be used.
- **Use Secure Network Connections**: It's important to be connected only to the trusted networks. Avoid the use of public Wi-Fi networks. More secure and trusted WiFi connections identified as "WPA or WPA2" requiring strong passwords should be used.
- **Install Apps From Trusted Sources**: Reading the user ratings and reviews can provide some clues about the integrity of the e-wallet app. The user must check for the e-wallet provider to be showing strong legacy of securely, reliably and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud).
- **Keep Login Credential Secure:** Avoid writing down information used to access the digital wallets in plain view or storing them in an unprotected file to avoid their misuse.
- **Create a Unique Password for Digital Wallet**: Use hard-to-guess password unique to the digital wallet to prevent against the risk of unauthorized access.
- **Stay vigilant and aware of cellphone's network connectivity status** and register for Alerts through SMS and emails: The user should not switch off his cellphone in the event when numerous annoying calls are received, rather answering the calls should be avoided. This could be a ploy to get him to turn off his phone or put it on silent to prevent him from noticing that his connectivity has been tampered with. The customer should realize that when he is not receiving any calls or SMS notifications for a long time against his e-wallet uses, he should make enquiries with his mobile operator to be sure about not falling victim to such scam.
- **Identify Points of Contact in case of Fraudulent Issues**: For any fraudulent activity occurring on the user's account in the scenarios like when phone is lost or stolen, an individual card stored in the wallet is lost or account has been hacked, appropriate points of contact for resolving the issues should be understood by the user. The user must completely understand the e-wallet providers contract terms and conditions.

Refrences:

http://www.cert-in.org.in/

Security of Micro ATM

Micro ATMs are Point of Sale (PoS) Devices that work with minimal power, connect to central banking servers through GPRS, thereby reducing the operational costs considerably. Micro ATM solution enables the unbanked rural people to easily access micro banking services in a very effective manner.

The basic interoperable transaction types that the micro ATM will support are:

1. Deposit
2. Withdrawal
3. Funds transfer
4. Balance enquiry and mini-statement.

The micro ATM will support the following means of authentication for interoperable transactions:

1. Aadhaar + Biometric
2. Aadhaar + OTP
3. Magnetic stripe card + Biometric
4. Magnetic stripe card + OTP
5. Magnetic stripe card + Bank PIN

Threats to Micro ATMs:

Data Vulnerabilities

With respect to POS data vulnerabilities, there are three specific areas that should be given attention including data in memory; data in transit; data at rest. Data in memory in this context is when the card track data is brought into the system at the POS system via a POI (Point of Interface or some other input device). Data in memory is nearly impossible to defend if an attacker has access to the POS system. Traditionally, data input into the POS system was in memory in clear text, which is what allowed, attackers¿ memory scrapers to be very successful. The way to minimize this risk is by encrypting the card data as soon as possible and keeping it encrypted to the maximum extend throughout its life within the system. Point to Point Encryption (P2PE) could be used to address the issue of encrypting data in memory.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can obtain victim's credit card number using a small electronicCredit Card device near the card acceptance slot and store hundreds of victim's credit card numbers.

Social Engineering

Social engineering involves gaining trust - hence the fraudster poses as a member of staff. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of micro ATM machine and requires assistance.

Best practices for users:

- Before using micro ATM, please ensure that there are no strange objects in the insertion panel of the ATM(to avoid skimming)
- Cover the PIN pas while entering PIN. Destroy the transaction receipts securely after reviewing.
- Change ATM PIN on a regular basis.
- Keep a close eye on bank statements, and dispute any unauthorized charges or withdrawals immediately.
- Shred anything that contains credit card number written on it.(bills etc)
- Notify credit/debit card issuers in advance for change of address.
- Don not accept the card received directly from bank in case if it is damaged or seal is open.
- Do not write PIN number on credit/debit card.
- Do not disclose Credit Card Number/ATM PIN to anyone.
- Do not hand over the card to anyone, even if he/she claims to represent the bank.
- Do not get carried away by strangers who try to help you use the micro ATM machine.
- Do not transfer or share account details with unknown/non validated source.
- In case of any suspected transactions or loss of cards, contact the service provider/bank immediately.

Best practices for service providers

- The micro ATM must not transmit any confidential data unencrypted on the network
- The micro ATM must automatically logout the operator and lock itself after a period of inactivity
- Keep all the micro ATM software ,application, anitvirus regularly dated
- Educate the customer about basic functionalities and security best practices.

Reference:

http://www.cert-in.org.in/

Further Reading
Micro-ATM standards available
at: https://www.idrbt.ac.in/assets/publications/Best%20Practices/MicroATMStandards_v1Draft.pdf

Security Guidelines for Point of Sales (POS)

Skimming is the transmitting of electronic data from a customer's credit or debit card account to another source for fraudulent purposes. Your customers may use a chip card or a magnetic stripe card. Some of these require that cardholders sign a sales voucher to confirm the sale. Others require that customers enter their PIN at the terminal. Criminals will try and place electronic equipment into the terminal or intercept the data communication path, in order to capture card data. If successful, this allows them to create false cards and perform fraudulent transactions. Here are some examples to illustrate tampering and skimming:

- POS terminals seldom have security stickers. Elsewhere, company stickers may be placed over screw holes to detect tampering. Criminals may remove these labels when compromising terminals, and replace it with their versions.
- Skimming devices concealed within POS terminals are invisible to merchant staff and cardholders.
- Use of key loggers to record key strokes.
- Criminal(s) enter the merchant location pretending to be service engineer(s).

Best practice security guidelines

Physical Location

Physical location has a considerable higher impact of you being targeted by criminals. These miscreants want high returns in terms of the number of captured credit and debit card details, in the shortest time. They want low risks of being caught, or of detection of the compromise. Criminals typically target isolated merchant locations situated near, or at, busy junctions to major highways. Locations that are open extended hours are especially attractive, since few staff members are on duty.

Change of location is not feasible for merchants. So it's important to understand the risks associated with your particular physical location and implement other guidelines for protection from attacks.

Terminal environment

Improvements in terminal security mean that compromises take longer time. However, due to the range and type of POS terminals in use, criminals can target merchant locations with 'older' and 'weaker' terminals.

To insert skimming devices, it's often necessary to take away POS terminals or swap existing terminals with compromised terminals. If your POS terminal is located at, or near the entrance to your store, consider providing additional security to prevent removal. For example, you could lock it in a stand permanently attached to a cash desk or sales counter.

Digital technology has resulted in smaller cameras. Criminals may hide cameras in imaginative ways, so their presence may not be obvious.

Staff

Speaking to staff members in relation to criminal activity is a sensitive topic. While we all consider our employees to be loyal, hardworking, and trustworthy, be aware that they are at risk from organized criminal gangs.

Be cautious if:

• Employees seem scared to answer questions or appear nervous. Be careful if they don't want to conduct regular checks of POS terminals.

- High-risk merchants should perform regular checks of all POS terminals—the surrounding environment must be part of daily routine.
- Maintain precise records of staff attendance, including any last minute changes. Keep these records for at least six months.
- Educate staff to be conscious of the types of attacks and associated risks.

Surveillance cameras

Surveillance cameras provide a deterrent to criminals. It's essential to keep such recordings for at least three months. Duty staff should not have access to surveillance cameras, past/present recordings and control equipment. Position surveillance cameras so that they record the area around the POS-PED device without recording entered PIN numbers.

Service personnel

When it’s necessary to call a service engineer, clearly agree on the time and date. Try and confirm the service engineer’s name.

If a service engineer (or a person claiming to be a service engineer) arrives unannounced at your merchant location, don’t allow access until you have verified his/her credentials. This must include contacting the vendor or service company to confirm their identity. All work undertaken by the service engineer must be written down in a report (retain it for at least six months).

Terminal connectivity

Modern terminals use a range of connectivity methods. Be aware that certain parts of transaction data are transmitted in clear text format. Since this data can be targeted by criminals, staff should understand and record all connections to the terminal. Note the entire cable path from the terminal to the point where it leaves your merchant location.

Wireless connectivity

Wireless connectivity permits terminals to be independent of cash counters. For example, the terminal can be taken to a table in a restaurant to allow customers to pay their bill without losing sight of their payment card. A criminal can easily steal, modify and return such a terminal without anyone realizing its absence. Track the number of terminals utilized each day, and devise a method to quickly identify who has the terminal at any particular time.

Bluetooth and Wi-Fi enabled Terminals

The terminal types mentioned above are usually either ‘Bluetooth’ or ‘Wi-Fi’ enabled. Although designed to operate over short ranges, criminals can intercept Bluetooth and Wi-Fi signals over significant distances—certainly beyond your merchant location’s walls. So enable the terminal’s security functions—apply all security updates and patches where necessary.

GPRS enabled terminals

Certain terminals connect to their host system via the GPRS (cellular phone) network. This allows merchants who are not at fixed locations (like at music concerts or festivals) to accept credit and debit card payments. Since there’s no fixed location, the merchant is responsible for ensuring the terminal’s integrity and security. Store such POS terminals securely when they are not in use.

Data security

Cybercrime is growing in diversity and sophistication—criminals are increasingly targeting merchant systems to obtain credit and debit card details. So understand how your systems work, and identify all possible points in the chain that could store data.

Often, merchants are not aware that sensitive data is stored in their systems. Therefore, merchants must adopt and follow the Payment Card Industry Data Security Standard (PCI-DSS) process and requirements.

To overcome POS terminal weakness and possibility of POS tampering, the steps that can be taken by acquirers, merchant and processors are:

• **POS equipment protection:** Keep a watchful eye on POS Equipment

•**Physical security:** Safeguard POS equipment and surrounding areas

• **Staff communication and education:** Train your employees on POS equipment tampering prevention

• **Prevent** or deter criminal attacks against POS terminals used at their location

• **Recognize compromised terminals** as soon as possible to minimize a successful attack's impact

Four Cyber Incident Scenarios Your Team Should Train For

Here are four scenarios you should train for and be ready to respond to in the event of a cyber security incident:

1. **Phishing Attacks**

The frequency of phishing emails and overall business email compromise (BEC) have gained momentum, especially as ransomware attacks have been on the rise. Ransomware now accounts for 27 percent of malware incidents, and 18 percent of organizations blocked at least one piece of ransomware in 2019, according to the Verizon Data Breach Report. Educating employees to practice due diligence is a first step and conducting faux phishing exercises can be a valuable teaching tool.

2. **Malicious Attachments and Malware**

It's just as important for your security team to know when malicious attachments and malware make their way onto the network as it is to avoid opening them. If malicious attachments make it through your filters and into your employee's in-boxes, or they visit malware infected websites, you need a plan in place – one that has been practiced – to be able to respond quickly and limit the damage.

3. **Password Requests and Other Suspicious Demands**

Cyber criminals can pose as employees, contractors, or third-party vendors to bait employees into divulging sensitive passwords and other access controls. Your security personnel should be trained on how to respond. You can test your incident response teams and employees by running exercises to simulate password requests from familiar sources such as the help desk or even executives, who are often spoofed.

4. **Unauthorized Users and Devices on Network and Cloud**

Computers and devices that haven't gone through proper authentication processes before joining your corporate network are perfect targets for attackers. Can your response teams not only identify attempts to connect to your network, but block them? Have you tested how quickly they can do this? If you're using cloud applications and infrastructure, are you monitoring access to environments like Amazon Web Services (AWS), Microsoft Azure, and Google, or to MS Office 365? Even if your organization is "just experimenting" with cloud platforms and services, you can be at risk for breaches and misuse if they're not properly configured for

optimal security, or if someone with authorized access sets up rogue accounts or operations on them.

Summary

These are just a few of the cyber incident scenarios you can use to test your incident response team’s readiness for a cyber incident. Practicing these on a regular basis can help your team be better prepared and identify any weaknesses before you’re in the midst of a crisis, saving you time, money, and peace of mind

Cyber Security Incident Handling

Best practices before, during and after security incidents

When a cyber-attack occurs, multiple activities may take place simultaneously, and this can be hectic when there is no coordination or proper incident handling procedures.

However, preparing in advance and establishing a clear and easy to understand incident response plan and policies allow the security teams to work in harmony. This enables them to focus on the critical tasks that limit the potential damage to their IT systems, data, and reputation in addition to avoiding unnecessary business interruptions.

Preparing an incident response plan

An incident response plan documents the steps to follow in the event of an attack or any other security issue. Although actual steps may vary according to the environment, a typical process, based on SANS (SysAdmin, Audit, Network, and Security) framework, will include preparation, identification, containment, elimination, recovery, notification of the incident, and a post-incident review.

In cident response process flow (based on NIST template) *Image NIST*

The preparation includes developing a plan with relevant information and the actual procedures that the computer incident response team (CIRT) will follow to address the incident.

These include:

- Specific teams and individuals who are responsible for each step of the incident response process.
- Defines what constitutes an incident, including what warrants what type of response.
- Critical data and systems that require more protection and safeguarding.
- A way to preserve the affected states of affected systems for forensic purposes.
- Procedures to determine when and who to notify about a security issue. When an incident occurs, it may be necessary to inform the affected users, customers, staff law enforcers, etc. but this will differ from one industry and case to another.

An incident response plan must be easy to understand and implement as well as align with other plans and organization policies. However, the strategy and approach may differ across different industries, teams, threats, and potential damages. Regular testing and updates ensure that the plan is valid and effective.

Incident response steps when a cyber-attack occurs

Once there is a security incident, the teams should act fast and efficiently to contain it and prevent it from spreading to clean systems. The following are the best practices when addressing security issues. However, these may differ according to the environment and structure of an organization.

Assemble or engage the computer incident response team

Ensure that the multi-discipline in-house or outsourced CIRT team has the right people with both the right skills and experience. Out of these, select a team leader who will be the focal person to give direction and ensure the response goes according to plan and timelines. The leader will also work hand in hand with the management and especially when there are important decisions to make as regards the operations.

Identify the incident and establish the type and source of the attack

Upon any signs of a threat, the IR team should act fast to verify if it is indeed a security issue, whether internal or external while ensuring that they contain it as fast as possible. Typical ways of determining when there is an issue include but not limited to;

- Alerts from security monitoring tools, malfunctions within the systems, unusual behaviors, unexpected or unusual file modifications, copying or downloads, etc
- Reporting by users, network or system admins, security personnel, or external third-party partners or customers.
- Audit logs with signs of unusual user or systems behavior, such as multiple failed login attempts, large file downloads, high memory usage, and other anomalies.

Varonis security incident automatic alert – *Image* *Varonis*

Assess and analyze the impact of the attack

The damage an attack causes vary depending on its type, effectiveness of the security solution, and the speed at which the team responds. Most often, it is not possible to see the extent of the damage until after completely resolving the issue. The analysis should find out the type of attack, its impact, and the services it could have affected.

Containment, threat elimination, and recovery

The containment phase includes blocking the attack from spreading as well as restoring the systems to the initial operation status. Ideally, the CIRT team should identify the threat and root cause, remove all the threats by blocking or disconnecting compromised systems, cleaning the malware or virus, blocking malicious users, and restoring services.

Notifying and reporting

The incidence response team does the analysis, responding, and reporting. They need to explore the root cause of the incident, document their findings of the impact, how they resolved the issue, recovery strategy while passing the relevant information to the management, other teams, users, and third-party providers.

Communications with external agencies and providers *Image NIST*

If the breach touches on sensitive data that require notifying legal enforcement authorities, the team should initiate this and follow the laid down procedures in their IT policy.

Conduct a post-incident review

Resolving an incident also offers lessons learned, and teams can analyze their security solution and address the weak links to prevent a similar incident in the future**.** Some of the improvements include deploying better security and monitoring solutions for both internal and external threats, enlightening the staff and users on security threats such as phishing, spam, malware, and others that they should avoid.

Nepal’s NIC Asia Bank incident response case study

Inadequate detection capability or response can lead to excessive damage and losses. One example is the case of Nepal’s NIC Asia Bank, which lost and recovered some money after a business process compromise in 2017. Attackers compromised the SWIFT and fraudulently transferred funds from the bank to various accounts in the UK, Japan, Singapore, and the USA.

Luckily, the authorities detected the illegal transactions but only managed to recover a fraction of the stolen money. Could there have been a better alerting system, the security teams would have detected the incident at an earlier stage, maybe before the attackers succeeded in the business process compromise.

Because this was a complex security issue involved other countries, the bank had to inform the law enforcement and investigative authorities. Also, the scope was beyond the bank’s internal incident response team and hence the presence of external teams from KPMG, the central bank, and others.

A forensic investigation by external teams from their central bank established that the incident may have been from insider malpractice that exposed critical systems.
According to a report, the then six operators had used the dedicated SWIFT system computer for other unrelated tasks. This may have exposed the SWIFT system, hence allowing attackers to compromise it. After the incident, the bank transferred the six employees to other less sensitive departments.

Lessons learned: The bank should have deployed an effective monitoring and alerting system in addition to creating proper security awareness among the employees and enforcing strict policies.

Conclusion
A well-planned incident response, good team, and relevant security tools and practices give your organization the ability to act fast and address a wide range of security issues. This reduces the damage, service disruptions, data theft, loss of reputation, and potential liabilities.

Cyber Security Assurance

Are you confident that you have the right cyber security countermeasures in place? Deploying sensible countermeasures can be an arduous and time-consuming task for any organization. Formal or informal cyber security assurance or certification can provide that extra layer of confidence to you and your stakeholders, demonstrating you are in alignment with best practice.

If your organization is looking to establish a systematic, risk-based approach to cyber security then our experts can help. We can conduct a comprehensive risk assessment covering processes, systems and assets. We offer mitigating, actionable recommendations.

DNV GL's cyber security assurances are aligned to ISO 27001 and ISO 31000

Securing your systems against cyber security risks

With an increasing convergence between IT and OT (operation technology), the OT domain is becoming more of a target for hackers, and the cyber security risk really pertains to safety and performance.

Cyber security evaluation and certification

Independent testing is essential to assess the actual cyber security exposure. DNV GL offers several cyber security test and assessment services. Within IT, we test according to the ISO 27001 standard and in OT, we offer testing in accordance with standards.

Benefits of cyber security assurance and evaluation:

- Alignment with best practice
- Improving stakeholder confidence
- Reducing operational risk following a cyber-attack
- Avoiding the exploitation of known or unknown vulnerabilities