**Phishing as a Risk (Damages from Phishing)**

Phishing steals identity and wrecks lives. It affects everyone, from a senior bank manager to a minor kid who may have never heard of internet scams. The worst part is that though phishing is now more than a decade old phenomenon, many people are not familiar with how it works and still fall victim to this scam.

Let us look at some of the ways in which successful phishing works.

* Using data for accessing victim’s account and withdrawing money or carrying an online transaction e.g. buying a product or service.
* Using data to open fake bank accounts or credit cards in the name of the victim and using them to cash out illegal checks, etc.
* Using victim’s computer systems to install viruses and worms and disseminating phishing emails further to their contacts.
* Using data from some systems to gain access to high value organizational data such as banking information, employee credentials, social security numbers, etc.

Now let’s see a few aspects to show us what impact or damages does phishing have on the victims.

**Financial Losses from Phishing**

It may not be easy for organizations to estimate financial damage incurred as a result of phishing. There are numerous factors to be taken into account when measuring the costs. Over the years, businesses have lost billions of dollars as a result of falling prey to phishing scams.

In 2015, spear phishing attacks alone caused a damage of an average of 1.5 million dollars per incident. According to a report in the first quarter of 2016 by the Ponemon Institute, successful phishing attacks can collect as much as up to 3.7 million dollars per attack. This happens even after specific security measures intended to counter such scams are deployed.

Regardless of this, more than 70% of organizations rely on traditional antivirus and antispyware programs and have very limited knowledge of how to secure their data. There is a need to understand that complete security requires extensive security measures to be adopted. Traditional programs may filter some emails or prevent a few attachments from opening, but if the message shows variation from the traditional scam messages, it may go undetected through the antivirus.

According to Federal Bureau of Investigation, large businesses have suffered severe financial damages to spear phishing emails where criminals impersonate company managers and order their staff to transfer funds to accounts which are actually controlled by the criminals themselves. They spoof email accounts of company executives and combine other phishing methods to make employees believe that the money transfer requests are actually sent from top executives or company vendors. The report also stated that the target of these criminals are usually businesses that deal with foreign suppliers or carry out regular wire transfers.

In January 2016, Austrian aircraft parts maker company FACC incurred a loss of approximately $54 million. The severe damage to its finances and reputation lead the company to fire its CEO in March the same year.

***Reducing the Financial Damages***

Organizations that are targeted by phishing scams or are potential victims for these attacks need to set up and maintain an extensive phishing protection plan. This may not completely remove the risk of phishing attacks, but it surely can minimize or prevent the direct costs altogether.

The plan should have strict guidelines that should direct the users to adopt specific response to every situation at every step. According to the report by FBI mentioned above, most of the financial damages are incurred within first 24 hours of the breach.

To reduce financial damages, organizations should take the following measures:

* Identify all stakeholders; assign and communicate their responsibilities.
* Develop and document a phishing protection and response plan which is compatible with current processes and procedures.
* Create effective communication processes, both internally and externally.
* Develop an escalation path for phishing response.
* Minimize negative customer experience and develop customer confidence in your online services.
* Hire the services of an anti-phishing team that is specialized in reducing phishing costs.

**Reputational Damages from Phishing**

It takes years of continuous customer satisfaction and fulfilling services to develop a brand name. All successful brands build on trust and earning that trust is no easy task. Don’t leave any opportunity to allow for potential attacks to your brand equity as it could cost you unrecoverable damage to your brand’s reputation.

According to a survey by Frost & Sullivan, about 71% of security professionals think of “brand protection” as the top priority. Every year, there are thousands of phishing attacks by cybercriminals on hundreds of top brands. All brands that do online business are targets for the criminals, but the ones with large amounts of customer data are highly fetched by hackers.

## *The Cost of Damaged Brand Reputation*

## Though financial damages may be recovered in a matter of time, it is the damage to a brand’s reputation that takes years to be recovered back to its original place. In case of an incident, customers are less likely to operate in the future with you.

## According to a study by Ponemon Institute, 31% of respondents said they would terminate their relationship with an organization if they receive a notification for a data security breach incident. Also, in case of third party supplier, a breach incident can lead to immediate termination of contract.

## An interesting thing is that in order for your company to deliver a bad message, it is not necessary for a consumer to provide their information and become a victim to a phishing scam. Instead, even receiving a phishing email that seems to have come from your company’s end can create a negative experience with a bad image in the customer’s mind and may contribute towards your brand’s bad reputation. Once the word gets out, more and more consumers start fearing identity theft and begin choosing your competitor instead.

## Minimizing Reputational Damage

## When it is about brand reputation, it always comes down to how much your customers trust you. Even if you have developed a strong consumer base and provide excellent products/services, remember that cyber criminals are also utilizing same amount of strength and hard work to extract your critical information. Success of your brand not only depends on the volume of sales. For the most part, it depends upon your ability to safeguard your customers and their information. Hence, it is their basic need to build a security infrastructure that allows your customers to safely conduct their business activities with you.

## In an event of data loss, the media scrutinizes and sensationalizes the news instantly and intensely. It is therefore advisable to devise an advance plan to handle such a situation. You have to give the exact facts and come up with a logical explanation of why and how it happened. This will show that you are in control of your situation. If you are not clear of the exact situation, do not let media point fingers at you until you have clear facts available.

## Do not blame a third party unless you are fully sure about it and your contract entitles you to do that. The most effective way to rebuild customer trust would be to apologize promptly for the incident and communicate how you intend to mitigate the damages.

**Denial of Service (DoS) implications of Phishing**

Businesses face more phishing scam emails and DoS attacks during the holiday season. In 2014, the famous Sony Pictures hack started with an employee clicking a phishing email. Two years from now, DoS attacks are even common than before. If someone wishes to harm your business, what better time it would be than to attack you at holiday season. It is the busiest time for businesses and can cause severe financial losses.

Though financial damage resulting from DoS attacks are an immediate loss and depend upon the industry, organizations that depend upon internet for carrying out business activities are the ones that mostly suffer. Other than revenue, financial loss may also include cost of investigation and attack response, customer support expenses, financial lawsuits, etc. Costs may also be incurred in the form of reputational damage and loss of productivity.

Online customers will always expect to have quick and easy access to information. A customer will lose interest in visiting a site if it is slower than its competitor’s site by more than 250 milliseconds, says Microsoft. Also, a customer who is unable to load a website for a particular information, purchase or a special service will eventually be dissatisfied.

While it is difficult to estimate the overall impact of a DoS attack on a business, there is no doubt in saying that it is always costly in the form of financial loss, customer turnover, reputational damage, etc.

***Avoiding the Damage***

Avoiding such incidents is possible, if not completely achievable.

Firstly, make sure that your public web and other services are either running in cloud, or are isolated in some other way from the real infrastructure. If a DoS attack happens, it only affects the webpage, and not the rest of the services.

Secondly, ensure that your public hosting service provider comes with an anti-DoS service. Having a sound endpoint protection will surely avoid a great many phishing email attempts which may otherwise be taken casually by an employee. In this regard, it is important to train your employees to be skeptic and learn how to respond to suspected phishing scams.

Thirdly, enable two-factor authentication for critical company services e.g. public profiles on Twitter and Facebook. With a two-factor authentication, a stolen password would not continue to be as dangerous. Even for services without two-factor authentication, keep a unique password and secure passwords in a container. Even if one unique password is stolen, it will not give complete access to the attacker to corporate identity.