Symantec

Cyber Security Services

Spear-Phishing and Health Care Organizations

How spear-phishing attacks are causing massive health care industry breaches and how to combat it

MSS Global Threat Team
Darian Lewis, Sr. Principal Threat Analyst
Eric Gonzalez, Principal Threat Analyst

Symantec

Contents

Symantec

Spear-Phishing and Health Care Organizations

Spear-phishing is one of the most prevalent cyber threats to organizations all over the world, attacking the human factor to infect computers, penetrate networks, and steal data. Anyone can fall victim to these attacks and the results can have company-wide implications.

The information here highlights the basics of spear-phishing email attacks and what you can do to protect yourself and your organization.

What is Spear-Phishing?

Phishing is an email-based social engineering attack that works by being logical, attempting to establish credibility or trust, or appealing to the recipient's emotions and values - it may be a combination of all of these. The goal of any phishing attack is to persuade a person to do something they might ordinarily not do – like clicking on a hyperlink in an email, sending out confidential information, or opening an attached document.

Spear-phishing is a highly-targeted phishing attack. It is tailored specifically for its intended victims using items they might normally see every day at work, like common names of people they might know, words that appear in their company's documentation, or other specific information that would lead them to believe it is a legitimate email. Most spear-phishing emails are very well researched and may be tailored to the specific recipient alone, a group inside the organization, or any employee.

Once the user has taken the steps they've been persuaded to take, criminals gain a foothold into your organization or get access to information that shouldn't be outside of the organization.

Spear-phishing is by far the most effective method to gain access, but why?

How do Spear-Phishing Emails Appear?

As mentioned, phishing, and spear-phishing emails in particular, are designed to be highly convincing. However, there may indicators that something isn't right.

If the sender isn't familiar to you but claims to be from your organization or an authority figure, you should ask your security department about the email. Here are some senders to be wary of:

- It could be someone you don't know personally within the organization
- It could be a person claiming government, law enforcement, or regulatory affiliation

What are URL Shorteners?

URL shorteners provide a convenient way to supply viewers with a more manageable URL. Take for example the Symantec Security Response Monthly Threat Report at https://www.symantec.com/security_response/publications/monthlythreatreport.jsp. By using bit.ly, a popular URL shortener or Google's URL shortener, you get http://symc.ly/1gQM83W or http://goo.gl/LAaPvF, respectively. Criminals will use shorteners to trick users into going to infected websites. If you need to re-expand a shortened URL use a web-based service like unshorten.it or urlex.org.

The tone of the email may not seem right to you or it may not fit the culture of your organization. It's either too formal or too casual compared to the normal email you receive.

- Suspicious attachments may be present with tempting or alluring file names or the filename might have multiple different extensions, such as "Receipt.pdf.scr" or "Salary_2014.zip.exe"
- There may be links in the email body designed to be deceptive or mismatched to the actual URL to which they go. The links may even use URL shorteners (*see sidebar*). Examples are link names like "microsoft.comserver.net". When you hover over the link with your mouse, you may see the actual link in your browser going to a different location or to a shortening service.

There may also be spelling, grammar, and formatting mistakes, indicating a non-native language speaker.

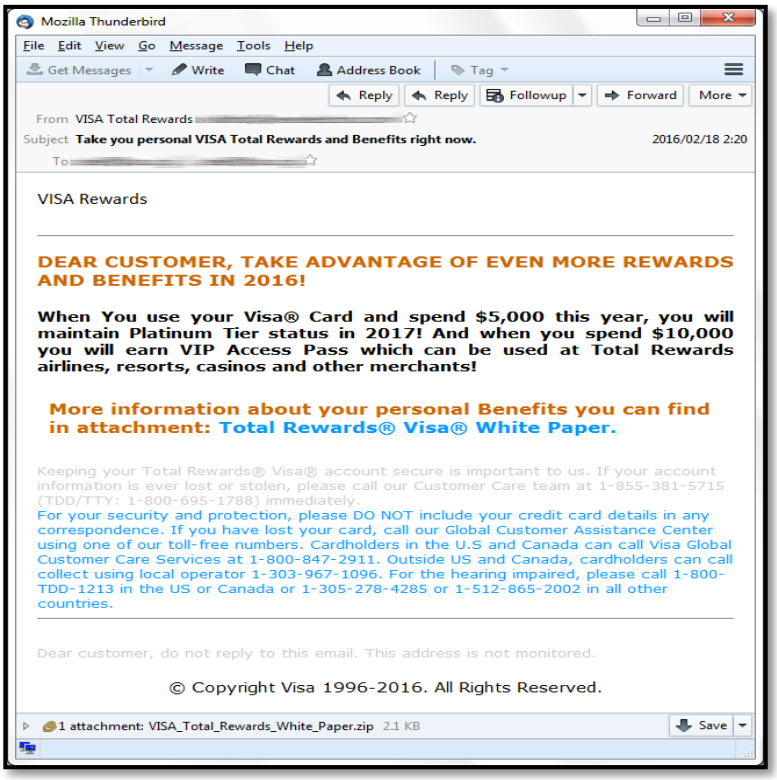


Figure 1: Fake spam leading to *TeslaCrypt*

A short video, Recognizing Phishing Attacks, explains some easy ways to recognize phishing emails. It can be seen at http://symc.ly/1pSRMeM.

What Happens with Phishing Emails?

In general, spear-phishing leads to installation of malware or theft of information. One spear phishing email may even lead someone to forward it to someone else within the company to give it additional credibility.

Malware

Malware is a persistent and pervasive threat with approximately 1 in every 244 emails containing malware. (*Source: Symantec ISTR)* How many emails pass through your organization every day? If you have 1,500 to 2,500 employees, then you may have seen more attacks, approximately 1 in every 76 emails contain malware. Many email appliances are getting better at detecting and stopping SPAM but spear-phishing is highly crafted and evade many of those technologies.

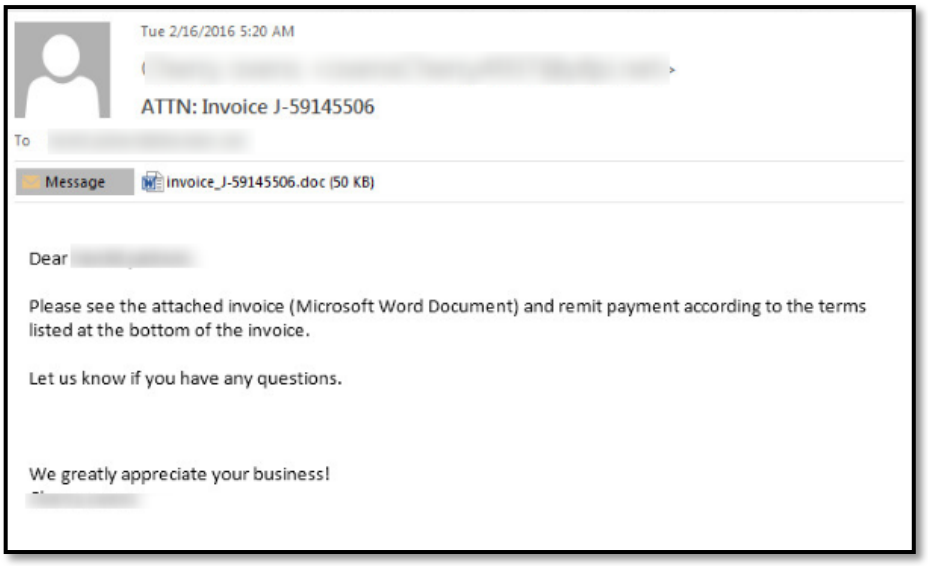
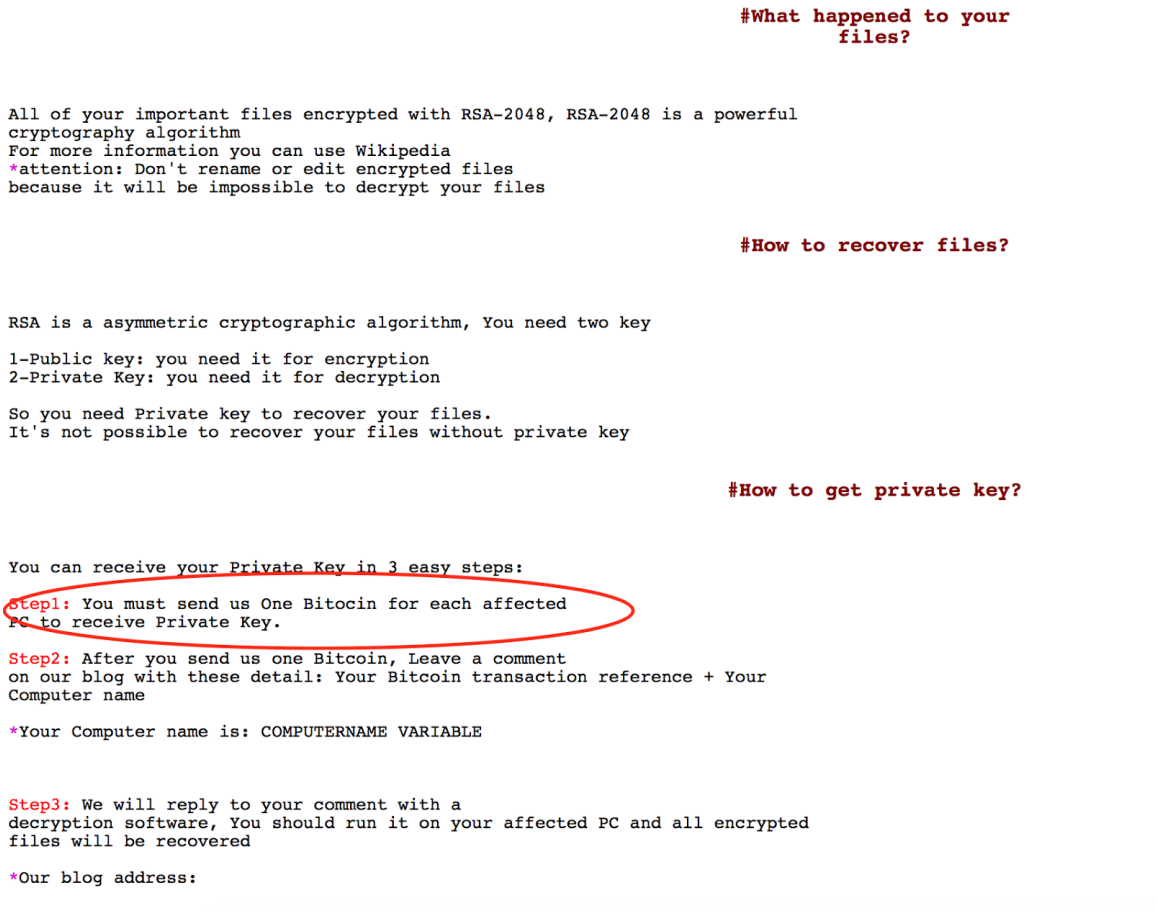


Figure 2: Phishing email leading to *Locky* malware

Ransomware

Ransomware is a relatively new type of malware that encrypts the hard drives of the victim computer. If an employee does open an attachment or run a program attached to an email, nothing may appear to happen immediately. Within a set timeframe that could range from an hour to a day, the computer will begin to show messages that indicate the computer is now being held hostage and that a ransom will have to be paid to get your data back.



#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files
because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitocin for each affected PC to receive Private Key.

Step2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

*Your Computer name is: COMPUTERNAME VARIABLE

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

*Our blog address:

Figure 3: Example ransomware message shown to users

The example phishing email in Figure 2 shows an example of a *Locky* delivering email. *Locky* has been used with increasing frequency against health care and related organizations. You may have seen the outcome of these attacks in the news where hospitals and medical centers have had to completely shut down all of their desktop computers and web-based systems to keep the *Locky* malware from spreading. It is not yet viral in nature, spreading computer to computer with its own malicious code. However, once *Locky* infects a file on a file share, other employees opening the file also become infected and it can quickly spread across departments and the entire organization.

The costs of a single *Locky* infection range from a few Bitcoins, a relatively untraceable cryptocurrency, to hundreds of Bitcoins to recover data.

Cryptocurrency

Cryptocurrency is a set of digital currency that uses cryptography to both create the units of currency, and to secure transactions using the units. Rather than using banks, crytpocurrency uses a decentralized (peer-to-peer) system and the rate of new currency creation is known to the entire system. Bitcoin is an open source cryptocurrency released in 2008 and has the largest cryptocurrency market share. The current value of one bitcoin fluctuates but is currently between $410 and $420 USD.

Symantec

What Should I Do If I Become Infected with Ransomware?

These are the steps you should take if you become infected with ransomware:

1. Activate your Incident Response system immediately and if you don't have an Incident Response team, Symantec has you covered. Call **855-378-0073** to immediately begin the triage process.

   Read more about Symantec Incident Response at https://www.symantec.com/services/cyber-security-services/incident-response
2. Contact law enforcement and your legal counsel for advice.
3. DO NOT PAY THE RANSOM.

Why not pay the ransom?

While that may be hard to accept when you're in the midst of a crisis, the best advice you can receive is **do not pay the ransom**. Even though the criminals may tell you they are going to double the ransom every day, do not pay it.

First, they are criminals. Giving them money funds additional criminal activity and encourages them to continue. Your ransom could be used to research and develop more advanced versions of ransomware. Second, they are criminals. There is no honor among thieves. They may not unlock your files even after you pay, or may leave a good deal of malware behind if they do. Third, they are criminals. If you pay, you will get added to the list of easy targets to hit again.

The best reason to not pay is because you already have a full backup and restore system in place as part of your compliance requirements. Your organization may lose data since the last backup, but your IT department should be able to help you get back to normal operations as quickly (and safely) as possible.

Data Theft

The criminals gained access to your data the moment the encryption malware was installed. The data is already lost and may be sold or traded on underground markets. Ransomware and Data Theft malware has been growing at an alarming pace.

The Symantec April 2015 release of the Internet Security Threat Report (ISTR), Volume 20 shows that 8.8 million ransomware attacks occurred in 2014, a rate of 24,000 per day. That number is up 113% from 4.1 million in 2013. This is a highly profitable endeavor for criminals who took in an estimated $34,000 in the first month of the *Cryptowall* release alone, and a $1M USD estimate over a six month period. This explains the recent explosion

in cryptographic ransomware as seen in figure 4.

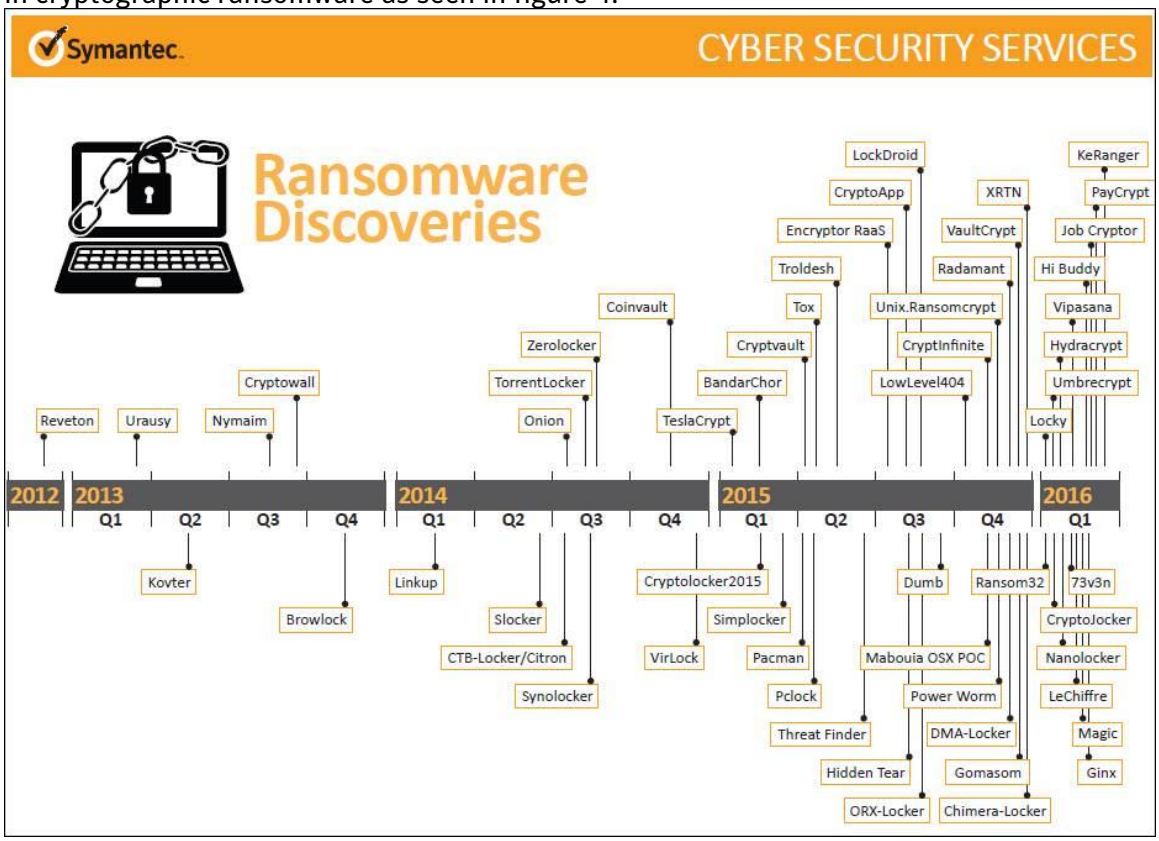


Figure 4: The ransomware timeline

What Can I do to Prevent Spear-Phishing Attacks?

Identifying spear-phishing attacks quickly can prevent the compromise of yourself and your organization. Notifying your IT security team of suspicious emails or suspected spear-phishing attack activity could limit exposure to others and keep sensitive data inside your organization.

If you believe you have a phishing email in your inbox:
If you believe you have been sent a spear-phishing email, please report it to your IT security team immediately. Symantec MSS stands ready to provide email analysis to extract key indicators of compromise (IOC). These IOCs can be leveraged with detection, to alert customers on future incidents.

If you've opened an attachment or clicked a link in what you suspect was a phishing email:
You should contact your IT security team and IT helpdesk as soon as possible given the sensitive and dangerous outcomes of many spear-phishing attacks. Due to the advanced and ever-evolving nature of this type of malware, an infected computer may not exhibit odd activity or trigger anti-virus alerts.

Provide Regular User Awareness Training

Training users to spot potential phishing activity is the best possible prevention. Technology can't always detect phishing attacks, but your fallback line of defense is your people. With Symantec Security Awareness Service, turn them into a resilient additional line of defense by providing them with valuable information on security best practices. Making all employees a part of the security conversation is the cornerstone of enterprise use awareness.

Symantec Phishing Readiness Service

By sending out well-crafted and relevant phishing test emails to employees regularly, you can detect problems and provide coaching. Symantec Phishing Readiness provides easy to use templates mirroring commonly used themes seen in phishing attacks such as social media and financially motivated messaging. By conditioning employees to look for certain cues in all emails that enter their inbox, they'll be able to more quickly and easily identify attacks and report them to security teams to close the feedback loop and thwart others from becoming victims.

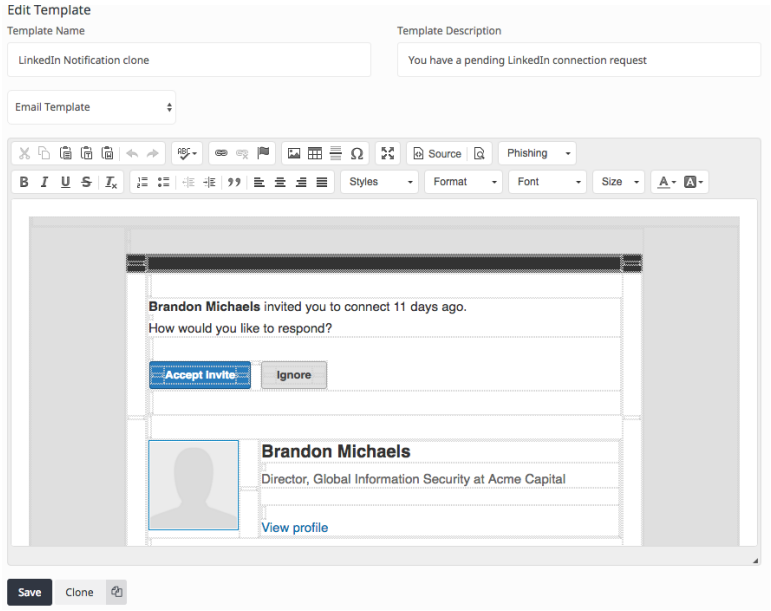


Figure 5: Phishing readiness LinkedIn template

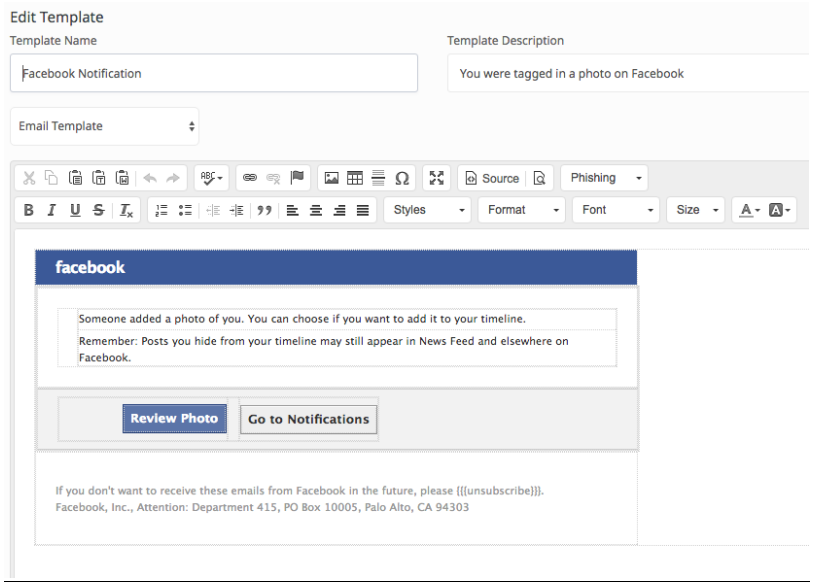


Figure 6: Phishing readiness Facebook template

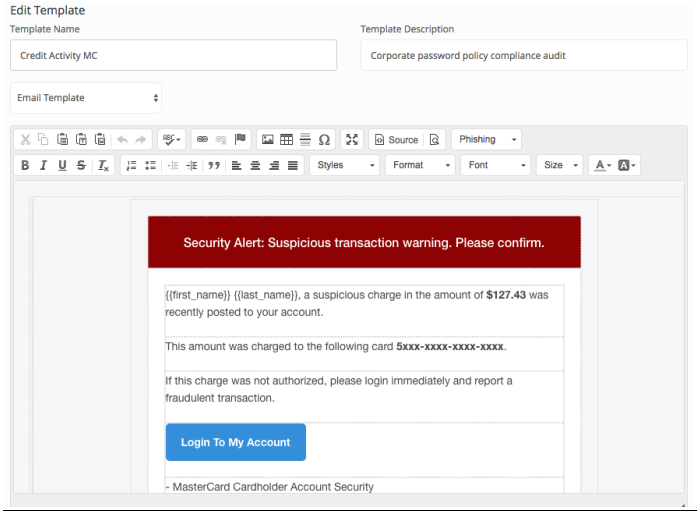


Figure 7: Symantec Phishing Readiness credit activity template

The templates are fully customizable for your organization to provide the most realistic training possible. This training will help employees distinguish phishing attempts from legitimate invitations.

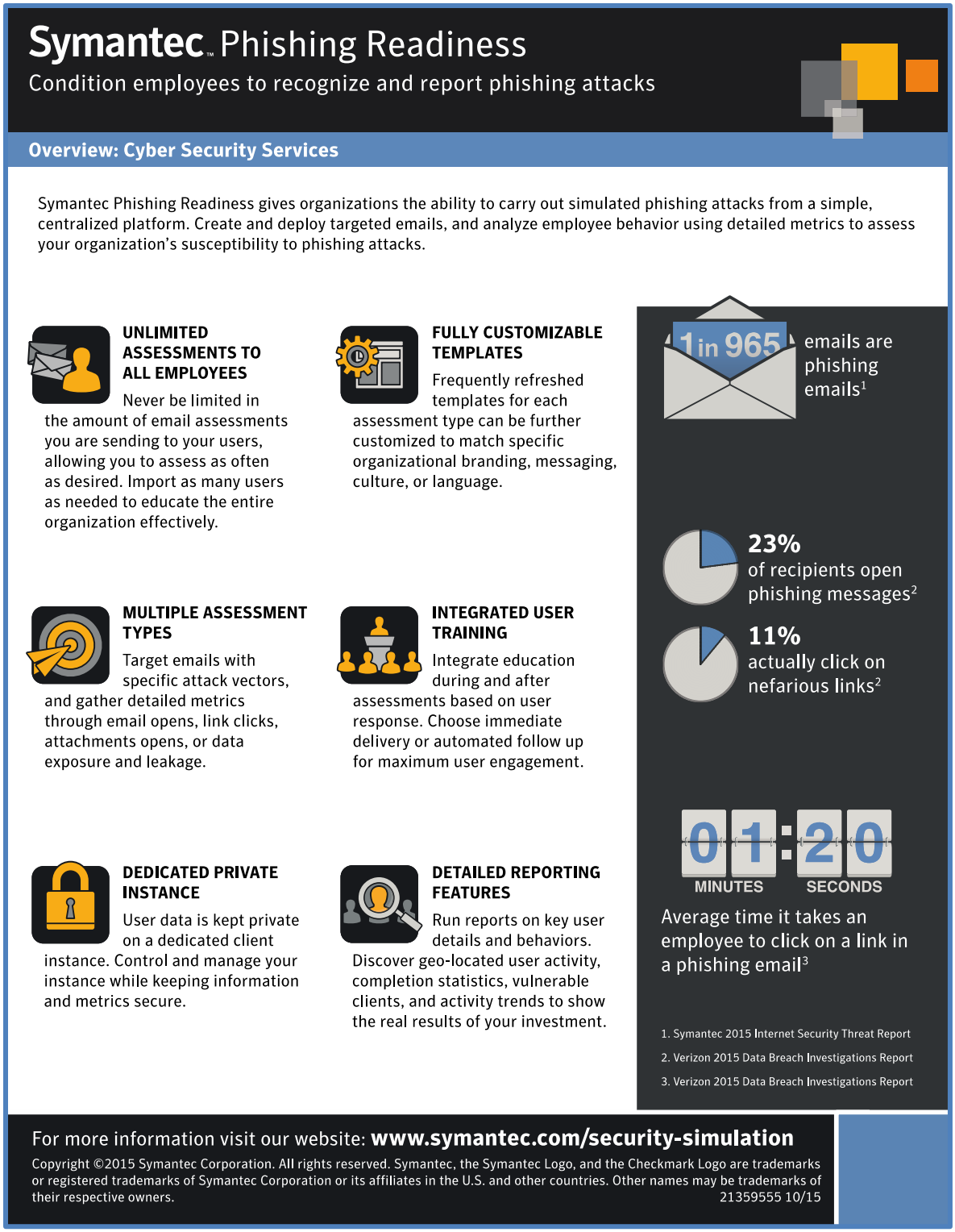


Figure 8: Symantec Phishing Readiness

What More Should I Be Doing?

Patch Where You Can

Security patches for known vulnerabilities cannot easily be applied to medical equipment. There are regulations in place to prevent any changes from being made that could impact the device's primary medical function. Medical equipment is often leased, with the lease agreement specifying that no modifications could be made by the users. If your healthcare organization does own the equipment, there is a good probability the equipment will lose its FDA certification (http://www.fda.gov/MedicalDevices/) if patches or ANY modifications are made. Since security patches typically cannot be applied to medical devices, security posture in healthcare must be increased in other parts of the organization.

Desktop computers can be patched dependent upon your organization's vulnerability management process. Make sure to keep up to date on patches for the most commonly vulnerable software and utilities. Make sure to remove any non-approved software and have endpoint protection like Symantec's Endpoint Protection, https://www.symantec.com/products/threat-protection/endpoint-family/endpoint-protection

Give Your Data Recovery and Business Continuity Plan a Health Checkup

Create and maintain a business continuity and disaster recovery (BC/DR) plan, a basic tenant of compliance. As part of the BC/DR plan, have layered backup storage. The most expensive storage for most immediately needed data (e.g. SAN copy), to the least expensive storage for archival records (e.g. tape) should be used. Your backup plan should be able to restore from any emergency with a minimum of data loss and a minimum of downtime to meet your data recovery point and data recovery objectives.

Make Sure You Are Reading Your Logs

You can only catch malicious activity if you can you see it. That means you have to be watching logs 24/7 to ensure you see malicious activity as soon as it happens. If you don't have the people, skills, or resources, utilize Symantec Managed Security Services to extend your team. You can read more about Symantec Managed Security Services at https://www.symantec.com/services/cyber-security-services/managed-security-services

Foster a Culture of Security in Your Organization

In the unfortunate event your organization suffers a ransomware incident, the real questions that need to be answered is how did this malware get into your organization and can you stop it from happening again?

Mandatory security education should be provided for everyone in the organization. Lock down USB ports and follow security best practices for endpoints as well. Also consider scanning and filtering on email servers to avoid the primary way malware is injected into any organization - phishing attacks.

References

2015 Internet Security Threat Report (Volume 20)
https://www.symantec.com/security_response/publications/threatreport.jsp

Symantec – "Spear Phishing: Scam, Not Sport"
http://us.norton.com/spear-phishing-scam-not-sport/article

Locky Ransomware on Aggressive Hunt for Victims
http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims

Spam Offering Fake Visa Benefits, Rewards Leads to TeslaCrypt Ransomware
http://www.symantec.com/connect/blogs/spam-offering-fake-visa-benefits-rewards-leads-teslacrypt-ransomware

Hospital Declares Internet State of Emergency After Ransomware Infection
http://krebsonsecurity.com/2016/03/hospital-declares-internet-state-of-emergency-after-ransomware-infection/