Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Enabling Social Networking Applications for Enterprise Usage

Copyright SANS Institute
Author Retains Full Rights

SANS ANALYST PROGRAM

*Sponsored by Palo Alto Networks*

# Enabling Social Networking Applications for Enterprise Usage

**A SANS Whitepaper – December 2010**

*Written by Eric Cole, PhD*

**Social Risks**

**Common Attack Pathway**

**Technical Risks**

**Enabling Humans**

**Enabling Technology**

# Introduction

The ability to stay in touch with friends and family members from anywhere in the world has millions of people caught up in the excitement of social networking. Because social networks are where the customers are, many enterprises are also turning to social networks as a free and powerful means of communication. Walmart, Cisco, Ford, and many other brand names utilize Facebook pages for sales, marketing, research, and customer service. In addition, many airlines are driving followers in Twitter by posting specials good only for the first one hundred customers (which encourages followers to track airfares closely and improves the chances of a buy).

Clearly there are benefits to be gained from social networking. The question is: How can you reap those benefits securely? Even if Facebook users have all of their security settings set to "friends only," do people really know who else is looking at their information? Social networking has no authentication, so anyone can claim to be Britney Spears or whoever they want to be when Twittering or Friending. In the words of Brad Paisley *"...there's a whole 'nother me that you need to see, go check out Myspace... I'm so much cooler online."*

Social networking sites have also become hotbeds for the distribution of malware. A report published in February, 2010, by Sophos showed a 70 percent increase in reports of users receiving malware and spam through social network sites over the previous year. Worms, phishing and Trojans take advantage of friend requests and other mechanisms of trust to get people's access information to spread and infect.

While there are many risks associated with social networks, there are too many benefits to be gained to simply ban social networks all together. The key is for businesses to define a secure social networking policy and to educate employees about the individual and organizational risks associated with using social networking sites. Organizations must also setup protective policies and technologies that prohibit unauthorized social networking applications, while monitoring approved applications for signs of abuse.

# Social Risks

Social networking sites are online platforms that help individuals find and build social relationships with other individuals on that same network. Some of the most popular social networking sites today include Facebook, MySpace, Twitter, Friendster and LinkedIn. Social networking sites are used for many reasons, including business networking, discovering individuals who share common interests, rediscovering individuals from one's past, and even for finding a life partner.

But with social networks come new risks to users and their places of employment. When using the social network at home, people can join new networks that phish for their account and access information or click "check this out" video links that infect their accounts and expose all their contacts on that social network. They can even get infections on their computers over social networks. If users are taking their lunch breaks to do all this from their work computers, their work computers and networks are equally vulnerable.

## Risks to Users

Many of these social network sites operate by allowing users to create profiles. A user's profile is a representation of the individual user, which can include as much personal detail as they desire. A user's profile can consist of many things including: their name, address, birthday, hobbies, pictures, etc. This profile information is shared among the user's community automatically (see Figure 1).

***"Use the settings to the right to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience."***

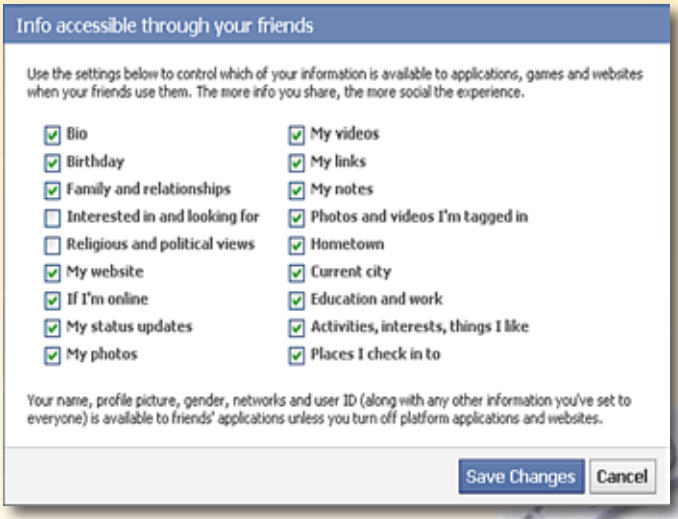


*Figure 1: Facebook Profile Information in Shared Applications Communities*

In addition to users exposing too much of their information, social networks have also become a top vector for phishing attacks. There have been many experiments showing that people will click on friend requests of people they don't actually know—maybe claiming to be a friend of a friend or maybe not even trying that hard. Once accepted as a friend, there is usually some type of phishing page that requires victims to join by filling out their information and passwords. With the phished credentials, the criminals take over the social networking account, its friend list, and so on. They then can use that data to phish the victim's contacts.

One of the most recent phishing attacks on Facebook was the FBAction messages circulating Facebook in late April, 2010.[1] The emails contained a link to a message sent from a "friend." If the user wanted to see the message, they had to click a link, which took them to the malicious login page. Once the user logged into their account through the malicious page, their credentials were captured and their account was compromised.

In addition, malware spread through social networks is a common attack vector included in today's advanced persistent threats (APTs). This spread of malware can be even more of a problem for employers because APTs that infiltrate network end points will attempt to spread further in the employer network.

## Risks to Business

Users of social networks don't usually understand the potential consequences of making their company information and titles public through their profiles. By so doing, they're posting data that's perfect for a spear phisher to use in crafting attacks that are convincing enough to get important personnel to click and follow malicious links.

Today's advanced threats use social networks to gather information about their targets. The data can be correlated to help an attacker crack a password or formulate some other form of exploitation against the individual or his or her place of business. Individual information may not seem damaging by itself, but what if it is combined with related information from eight co-workers also posting to their social networks?

[1] http://isc.sans.edu/diary.html?storyid=6292

The other threat to organizations is the use of social networks as avenues for data leakage. The point of social networks is for users to share, but sometimes users share too much information. An employee may be posting sensitive information about certain projects he or she may be working on or a new pre-launch product that employee is excited about. They may be voicing concerns about the company's financial status, talking about a big pay bonus or a change that involves them and the organization's structure, or even a scandal/investigation that affects the organization. Or, how about in the case of Linked In, where the employee's business information and business relationships and contacts are visible? This type of information can give competitors (and spear phishers) a great advantage.

Deliberate insider abuse is also a problem when a company allows social networks. Malware uses social networking traffic to set up command and control channels and also to export sensitive information by hiding it in ordinary traffic. This is also a common method used by insiders. In February, CA Technologies released its State of Internet Security report warning about how social networking sites are being used to recruit 'moles' for cyber espionage and terrorism.[2] If the proper measures are not put in place, a rogue employee can easily copy any sensitive information and message it to a friend or post it on someone's wall.

[2] www.ca.com/files/SecurityAdvisorNews/h12010threatreport_244199.pdf

# Common Attack Pathway

It's been established that social networks are now commonly used to propagate phishing, malware, spam, APT, botnets, fraud, and more. Here's how social networking attacks usually work:

- **Lure them in.** Attackers utilize phishing attacks, which lure victims to a malicious login page, such as FBAction case.
- **Spread through the social network.** Once attackers gain a user's credentials, they use the exploited account to social engineer other Facebook users into clicking links and giving over their accounts. The attacker simply impersonates the user and sends a malicious message or link to all of the user's "friends."
- **Takeover other personal and business accounts.** People have the bad security habit of using the same usernames and passwords for many different accounts. So, once an attacker compromises the login information to one account, he or she can compromise other accounts using the same credentials.

  Unfortunately, in order to create a profile with Facebook, a user must supply an email address and password. The email address then becomes the Facebook username when logging into the account. So if an attacker compromises a Facebook account with the username: JohnSmith@gmail.com and the password: 'jsmith,' a logical next step for the attacker would be to try compromise the Gmail account with that same password or derivatives thereof. Now, not only are all of John Smith's Facebook friends at risk, but also all of his Gmail contacts.

  If John Smith uses his work account, this is a direct threat to his place of employment. If he used another email account but listed his workplace, the combination of his name, workplace and password could be enough to exploit his place of business.
- **Spread to other devices.** This can occur in small home networks, but is a larger problem for the employer network.

# Technical Risks

Cybercriminals are focusing their attention on exploiting social networking sites for the large payoff they get when exploiting one account to phish others. They are also using social networks (including small gaming networks) to spread malware. Here are some examples of technological exploits being conducted within social networks:

1. **Banking malware.** Social networks in 2010 were heavily leveraged to spread the Zeus Trojan, a piece of malware that captures and exploits online banking information for small business accounts that use automated transfer services. URLZone, another Trojan designed to steal money from exploited users' bank accounts, utilizes social networking. The URLZone Trojan is an advanced piece of malware that actually alters the HTML coding of online bank statements in order to hide from the user the money transfer from the exploited account.

2. **Botnets.** Social networking sites have also contributed to an increase in botnets. A recent exploit for social networking sites is the Koobface worm, which infects Windows, Mac OS X, and Linux systems. The purpose of the Koobface worm is to collect login information and other credentials from a system. The worm spreads through Facebook messages and wall posts that urge users to go to a third party website and download a critical "update" (malicious code) for Adobe Flash Player. Downloading and executing the file infects their system. Once the worm infects a system, that system then becomes a zombie system in the botnet.

3. **Third-party applications.** Another social networking attack vector is in third party social networking applications.[3] The problem is that most third party applications do not undergo appropriate security testing or vulnerability scans. Many times these applications contain vulnerabilities or poor programming techniques, which could easily be exploited by an attacker. Because many users assume a high level of trust, they often install or click on interesting sounding applications not knowing that there could be hidden features or security holes. Some of these applications, including one of Facebook's most popular applications, Farmville, also distribute personal user information to third party websites, where it is distributed to advertising firms and Internet tracking firms.

   Also, in the case of shared applications such as games, the full user profile, unless specifically changed through multiple steps, is shared with everyone else using those shared applications.[4]

[3] www.facebook.com/apps/directory.php?
[4] www.eff.org/deeplinks/2010/08/how-protect-your-privacy-facebook-places

4. **Locations.** Facebook: Places allows users to "Check-In" at restaurants, stores, movie theaters, and so on. When a user "checks-in" to a certain place, usually with a mobile phone, the user's friends and friends of friends (and those using shared applications) can see when and for how long the user will be away from home—important information to any local criminal interested in burglary. In addition, when a user checks into a place, his or her location is viewable to all others checked into a location, even if they are not the user's friends.

   If it is a work employee checking in and the company is the target, compromising a protected system may be as easy as meeting up at a technology event and handing a key employee a USB stick (which the employee innocently plugs into a company computer inside a secure network). Facebook and other services that provide location-based check-in have privacy settings, but they are manual and involve many steps.

5. **URL posting.** Often times, social networking applications, such as Twitter, will allow users to post URLs to websites for other users to click on. This allows users to share information, videos, and other items, without typing in or posting excessively long URLS they're attached to. So, for example, with Bit.ly and TinyURL services, a user simply copies and pastes the desired URL into the Tiny interface and then creates an alias for the URL. This gives attackers the ability to direct a user to a malicious website by naming the link "sneakybadguys.net" to "HILARIOUS YOUTUBE VIDEO."

There are many other instances of malware affecting social networking sites, some of which have not even been identified yet. But all of them will be problematic for organizations participating in social networking, as well as their employees that do so.

# Enabling Humans

When it comes to social networking and security, it is important to avoid the extremes. Allowing full access with no restrictions to social networking sites is dangerous. However banning social networks can also be a bad business move, not to mention it will create new risk because users will find ways to do it without the IT staff's knowledge or protection. Other than losing a valuable enterprise tool, organizations still have employees that use these types of websites outside of work, and what they divulge there can still be damaging.

This means that the best way to enable social networking with security is through education. Organizations should create social networking security programs that educate employees about appropriate, safe uses and about the dangers of social networking sites. It is important that the program emphasizes the importance of protecting personal information as well as company private information.

## Settings

Employers must help employees learn and understand their privacy settings. For example, unless privacy settings are manually adjusted, all profile information, posts, changes, locations and friend data is automatically viewable to friends and friends of friends in their Facebook communities. It is also important to note that making updates or subtle changes to a profile could cause all the profile settings to change. It is not a bad idea to create a separate account and use it to login in with periodically to see what personal information your primary account is giving away.

Under "Account," users have privacy settings with buttons they can click to customize. Under customization options, most people will click "friends only" for minimum privacy, and "only me" for strictest privacy. For example, someone worried about their location being tracked by the wrong people can use "check me into places," but set up a small list of people allowed to see that information. For strictest privacy, they should not allow anyone to check them into places and make their location viewable to "only me." Facebook privacy settings are shown in Figure 2.

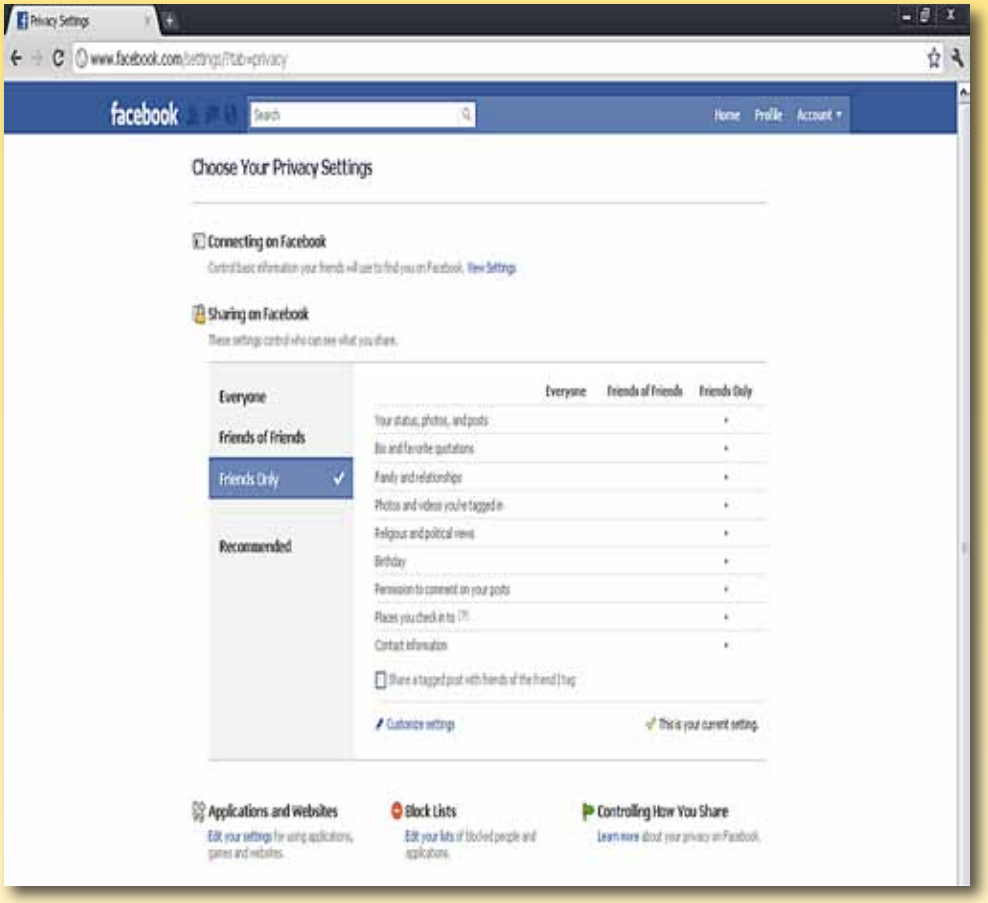


*Figure 2: Customized Privacy Settings on Facebook*

Unfortunately, at least in the case of Facebook, not all these settings carry over to applications shared with friends. For example, regardless of your primary privacy settings, location data is sent to everyone sharing that application (and their friends), unless locations is disabled. To adjust private data shared with applications requires going back to the privacy page and, in another location, on the lower left, a larger window appears with multiple options for applications, as shown in Figure 3.

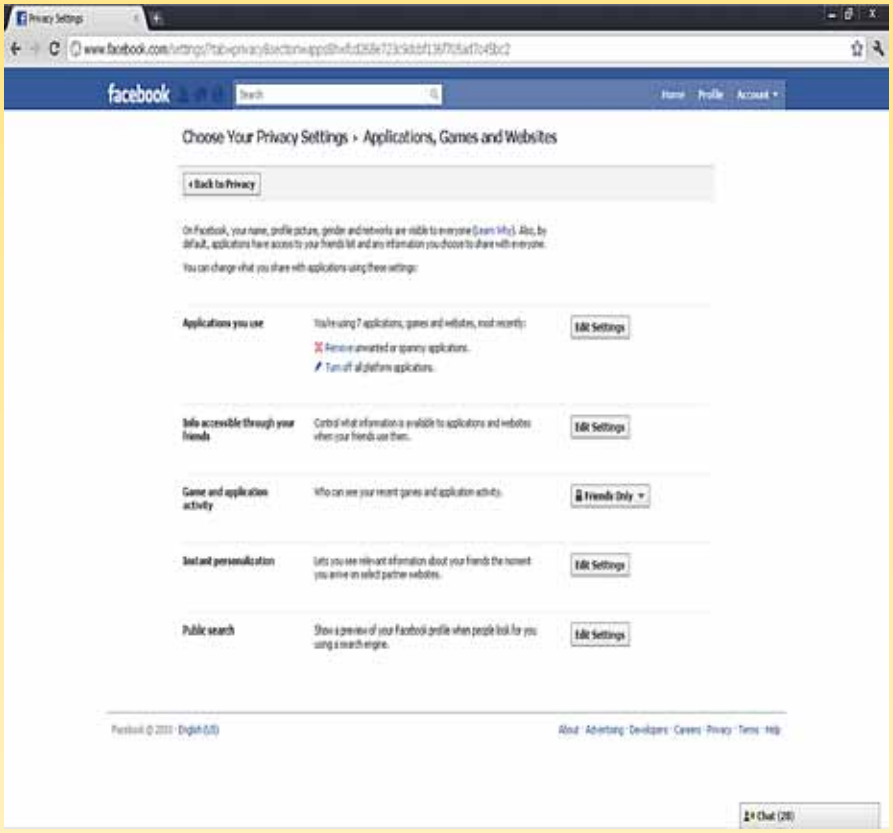


*Figure 3: Facebook Privacy Settings for Shared Applications*

## Postings and Messages

Other education points should protect against malware hidden in URL posts, malicious friend requests, messages and other ways malware and phishing spreads. Because of the many attack vectors presented in social networking, education should also emphasize the importance of being skeptical of all types of interactions requesting that the user click links or filled out forms. Everything is not always what it appears to be: even 'CHECK OUT THIS VIDEO' messages posted on friends' sites could have malicious payloads.

It is also critical for employees to be careful of what work information they post. Saying you had a stressful day is OK, but saying you had a stressful day because you lost a $30 million contract crosses the line. It might not seem like a big deal, but this type of information is absolutely intellectual property and can be useful to competitors in takeovers and other such situations. Even with the strictest security settings, you should assume someone you wouldn't want to read what you post can do exactly that. So limiting information can also help. For example, do you really even need to list your employer and location in your profile?

# Enabling Technology

In order to protect against these advanced attack methods utilizing social networking, organizations need technology policies to minimize the risk of intrusion and data theft through these applications. For best protection, policy should include the following:

- **Control application usage.** Organizations should start by allowing only approved social networking applications and disallowing unnecessary application traffic types. New identification technologies allow organizations to control Facebook functionality, users, and content, including which Facebook functions are operating on the network. This technology can be used to locate and identify risks associated with the Facebook operations.
- **Monitor approved applications for signs of abuse.** Watch approved traffic to and from social networking applications for signs of data leakage, such as large and encrypted files being posted and sent over social networking mail. Also monitor for command and control signals or unusual spikes in outbound social network traffic or traffic hopping between ports it shouldn't be hopping between.
- **Monitor users.** Most employees sign an Internet security contract explaining their lack of privacy when using organizational resources (i.e. computers/networks). This type of contract allows an organization to monitor all network traffic.
- **Manage risk.** Security is all about managing and controlling risk. There might be some unsafe social networking features that are needed even if they could cause a compromise. In this case, you might allow the feature, but it should be configured as securely as possible and scanned continuously for attempted exploitation, access, changes, etc.
- **Control plugins.** New advancements in firewall technology have given enterprises the ability to control Facebook Social Plugins. By approving and blocking certain plug-ins and their traffic at the firewall, organizations have the ability to control what confidential information is shared with third party applications.
- **Control and monitor access.** Microsoft Active Directory and other directory services in use should link Facebook functions to certain users or groups. This allows an administrator to differentiate between what applications different users can and should be using.
- **Monitor social networking application behaviors.** Monitor and block unauthorized uses of or changes to the social networking application, its plugins and other features. Watch for unusual traffic destinations or sizes, or unauthorized users.
- **Monitor and control corporate used social networking sites.** All of these rules apply also to the social networking site owned and operated by the place of business. This includes monitoring for changes made to the site or its applications, the existence of malware installers on the site, and user communications.

# Conclusion

Social networking is a valuable outreach resource for organizations, but it is accompanied by added risk. Just as the risks of social networking are both human-based and technology-based, so, too are the measures needed to enable secure social networking while instilling safe usage habits that carry outside the organization.

Social networks provide a vast amount of information, some of which can be used by an attacker to exploit an individual at his or her place of employment. Once that information is gathered, an attacker can use social networking sites to trick a target into installing malware that could spread to the organization.

In order to protect both employees and the organization, it is important to educate employees about the dangers of posting too much personal information on social networking sites, as well as the dangers of phishing and malware. Technical controls are just as critical, including advanced firewall and application capabilities (whitelisting, fine-grained controls), monitoring, and other controls.

By developing social networking policies, training/educating employees, and instituting proper technical controls, organizations can make use of social networking more secure for their employees and their networks.

# About the Author

**SANS Faculty Fellow, Dr. Eric Cole,** is an industry-recognized security expert and founder of Secure Anchor Consulting, where he currently performs leading-edge security consulting, provides expert witness testimony, and works in research and development. Cole's IT focus areas include perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Cole has a master's degree in computer science from New York Institute of Technology and a PhD from Pace University, with a concentration in information security. He is the author of several books, including *Hackers Beware, Hiding in Plain Site, Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards.

*SANS would like to thank this paper's sponsor*

the network security company™

Last Updated: December 18th, 2014

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Brussels 2015** | **Brussels, BE** | **Jan 26, 2015 - Jan 31, 2015** | **Live Event** |
| **SANS Dubai 2015** | **Dubai, AE** | **Jan 31, 2015 - Feb 05, 2015** | **Live Event** |
| **Cyber Threat Intelligence Summit & Training** | **Washington, DCUS** | **Feb 02, 2015 - Feb 09, 2015** | **Live Event** |
| **SANS Scottsdale 2015** | **Scottsdale, AZUS** | **Feb 16, 2015 - Feb 21, 2015** | **Live Event** |
| **10th Annual ICS Security Summit** | **Orlando, FLUS** | **Feb 22, 2015 - Mar 02, 2015** | **Live Event** |
| **SANS Secure India 2015** | **Bangalore, IN** | **Feb 23, 2015 - Mar 07, 2015** | **Live Event** |
| **SANS DFIR Monterey 2015** | **Monterey, CAUS** | **Feb 23, 2015 - Feb 28, 2015** | **Live Event** |
| **SANS Munich 2015** | **Munich, DE** | **Feb 23, 2015 - Mar 07, 2015** | **Live Event** |
| **SANS Cyber Guardian 2015** | **Baltimore, MDUS** | **Mar 02, 2015 - Mar 07, 2015** | **Live Event** |
| **SANS Northern Virginia 2015** | **Reston, VAUS** | **Mar 09, 2015 - Mar 14, 2015** | **Live Event** |
| **SANS Secure Singapore 2015** | **Singapore, SG** | **Mar 09, 2015 - Mar 21, 2015** | **Live Event** |
| **SANS Abu Dhabi 2015** | **Abu Dhabi, AE** | **Mar 14, 2015 - Mar 19, 2015** | **Live Event** |
| **SANS Secure Canberra 2015** | **Canberra, AU** | **Mar 16, 2015 - Mar 28, 2015** | **Live Event** |
| **SANS Security East 2015** | **OnlineLAUS** | **Jan 16, 2015 - Jan 21, 2015** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |