



ماهنامه آگاهی از امنیت اطلاعات برای شما

# امنیت سایبری، یک حرفه

## مقدمه

امنیت سایبری چیزی است که هر روزه در اخبار درباره آن می‌شنویم و می‌بینیم که سازمانها و دولتها در سراسر دنیا مدام در حال هک شدن هستند. درخواست همکاری بسیار زیادی برای افراد دوره دیده در زمینه امنیت سایبری وجود دارد تا به کمک آنها بتوان در مقابل رشد بسیار زیاد اینگونه تهدیدها دفاع کرد. در حقیقت، حدود 3 میلیون درخواست شغل در این خصوص در سراسر دنیا وجود دارد. آیا شما برای خود شغلی با عنوان امنیت سایبری حرفه ای (Cybersecurity professional) در نظر گرفته اید؟ این حرفه با رشد سریع و بسیار پویا، شامل تعداد زیادی تخصص های انتخابی نظیر کشف جرم (secure coding، Incident Response، critical infrastructure، end point security، forensic) و آگاهی و آموزش میباشد. علاوه بر این با انتخاب حرفه ی امنیت سایبری شما قادر خواهید بود در هر کجای دنیا با مزایای فوق العاده مشغول به کار شوید و این فرصتی برای ایجاد تفاوت های واقعی خواهد بود.

## آیا برای کار در این حرفه نیاز به دارا بودن مدرک علوم کامپیوتری است؟

به هیچ عنوان. بعضی از بهترین متخصصان امنیتی دارای پیشینه های غیر فنی میباشند، از بین این متخصصان افرادی با رشته زبان انگلیسی گرفته تا رشته های مانند پزشکی، تاریخ، مکانیک خودرو، هنر و یا حتی مادران خانه دار دیده میشوند. نکته کلیدی اشتیاق به یادگیری است- تمام امنیت سایبری در دانستن نحوه کار تکنولوژی ها خلاصه میشود. زمانی میتوانید تکنولوژی را بهتر امن کنید که بدانید آن تکنولوژی چگونه کار میکند.

## چگونه شروع کنیم

اگر نمیدانید از کجا شروع کنید تکنولوژی های مختلف را بررسی کنید و ببینید کدامیک برای شما جالب تر است.

کدنویسی: اصول برنامه نویسی را بیاموزید، میتوانید با پایتون، HTML و یا Javascript شروع کنید. برای این کار میتوانید با گشتن در سایتهای آموزشی و یا با مطالعه کتاب های آموزشی مبتدی کار خود را شروع کنید.



سیستم ها: اصول اولیه مدیریت یک سیستم عامل نظیر ویندوز و یا لینوکس را یاد بگیرید. کار با لینوکس استارت خوبی است. یادگیری مدیریت لینوکس از طریق خط فرمان (command line) مهارت شما را در این مسیر افزایش خواهد داد.



برنامه های کاربردی: نحوه پیکربندی، اجرا و نگهداری برنامه های کاربردی نظیر سرور وب (web server) و یا سرور DNS را بیاموزید.



شبکه بندی: نحوه عملکرد یک شبکه را بیاموزید و با جمع آوری و تحلیل ترافیک های شبکه ای بین تجهیزات و کامپیوترها یاد بگیرید که چگونه این تجهیزات با یکدیگر صحبت میکنند. به احتمال زیاد در منزل خود شبکه ای از تجهیزات متصل به هم را داشته باشید و این کار میتواند بسیار لذت بخش باشد.



یک روش بسیار عالی برای یادگیری این است که آزمایشگاه خود را در منزل راه اندازی کنید. این کار بسیار راحت است چرا که شما میتوانید چندین سیستم عامل مجازی را در یک کامپیوتر فیزیکی ایجاد کنید و یا با استفاده از منابع ابری (Cloud resources) نظیر Amazon AWS و یا Microsoft Azure آزمایشگاه مورد نظر خود را راه اندازی کنید. با اجرا شدن و بالا آمدن سیستم عامل میتوانید کار کردن با آنها را شروع کنید و هر چیزی که میتوانید یاد بگیرید. گزینه دیگر ملاقات و کار کردن با دیگران در زمینه امنیت سایبری است. در کنفرانس های محلی مرتبط با امنیت سایبری (که اصطلاحاً con گفته میشود) شرکت کنید. معمولاً در شهرهای بزرگ چندین رویداد از این دست در سال برگزار می شود. یک مجموعه شناخته شده از رویدادهای امنیت سایبری که برای کمک به افراد مبتدی طراحی شده Bside نام دارد. سخت ترین بخش پیدا کردن اولین رویداد یا ملاقات است. زمانیکه در اولین رویداد شرکت کردید، ارتباطات و فرصت های شما به طور چشمگیری افزایش خواهد یافت. گزینه های دیگری نیز برای یادگیری وجود دارد که شامل ویدئو های یوتیوب، انجمن های آنلاین و یا عضویت در وبلاگ های افراد متخصص امنیت است. در آخر اینکه برنامه های متعددی برای کمک به شما بعنوان مبتدی وجود دارد تا بتوانید حرفه خود را شروع کنید، از جمله این برنامه ها میتوان به CyberTalent Immersion و Cyber Aces و Cyber Academies و Cyber Patriot programs اشاره کرد.

در خاتمه اجازه ندهید که رشته تحصیلی یا سابقه کاری قبلی شما مانع پیشرفت شما در این خصوص شود. مهم نیست که سابقه کاری قبلی شما چه چیزی است، با هر پیش زمینه کاری که دارید، چیزی منحصر به فرد و خاص که مورد نیاز امنیت سایبری است را با خود خواهید آورد. کلید آن اشتیاق به یادگیری است. هنگامی که شما شروع به توسعه مهارت های خود میکنید و با دیگران در این زمینه دیدار میکنید، فرصت های جدید به سراغ شما خواهد آمد.



## سر دبیر مهمان

هیدر ماهالیک (@heathermahalik) مدیر و مهندس کشف جرم (Forensic) در ManTech Card و همچنین استاد ارشد و نویسنده دوره های SANS Digital Forensics and Incident Response (DFIR) میباشد. وی بمدت 17 سال در زمینه امنیت سایبری مشغول به کار بوده و شیفته این شغل میباشد. وبلاگ او از طریق [www.smartforensics.com](http://www.smartforensics.com) در دسترس همگان است.

## منابع

رویداد Bside:

<http://www.securitybsides.com>

برنامه CyberTalent Immersion Academies:

<https://www.sans.org/cybertalent/cybersecurity-career/seekers>

برنامه Cyber Aces:

<https://www.cyberaces.org>

برنامه Cyber Patriot:

<https://www.uscyberpatriot.org/>

برنامه Cyber Patriot:

[www.codeacademy.com](http://www.codeacademy.com)

OUCH! توسط برنامه «زندگی امن» موسسه SANS تحت مجوز Creative Commons BY-NC-ND 4.0 منتشر و توزیع شده است. اجازه توزیع این خبرنامه به شرط ذکر منبع، بدون تغییر محتوا و نداشتن مقاصد تجاری داده میشود. برای اطلاعات بیشتر، لطفاً با [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter) تماس بگیرید. هیأت تحریریه: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | ترجمه شده توسط: سعید میرجلیلی، مجید هدایتی