How to Hire an Ethical Hacker

When it comes to protecting your business, you can never be too careful. That's why in an age of DDoS attacks and phishing, it can help to have some insurance on your side. Ethical hackers, sometimes referred to as 'white hats,' possess...

Part 1 of 3:

Filling the Position

1. 

Evaluate the risks of going unprotected. It may be tempting to try to save money by sticking with your existing IT team. Without specialized backup, however, your company's IT systems will be vulnerable to attacks that are far too sophisticated for the average computer whiz to catch. All it would take is one of these attacks to do serious damage to your business's finances—and reputation.[1]

1. All told, the average cost of securing and cleaning up an online data breach is around $4m.[2]
2. Think of hiring a white hat as taking out an insurance policy. Whatever their services command is a small price to pay for your peace of mind.

2. 

Identify your company's cybersecurity needs. It's not enough to simply decide that you need to beef up your internet defenses. Come up with a mission statement outlining exactly what you hope to accomplish by hiring an outside expert. That way, both you and your candidate will have a clear idea of their duties going in.[3]

1. For example, your financial company might need increased protection from content spoofing or social engineering, or your new shopping app may put customers at risk of having their credit card information stolen.[4]
2. Your statement should function as a kind of reverse cover letter. Not only will it advertise the position, but also describe the specific experience you're looking for. This will allow you to weed out casual applicants and find the best person for the job.

3. 

Be prepared to offer competitive pay. Having an ethical hacker on your side is a wise move, but it isn't a cheap one. According to PayScale, most white hats can expect to pull in $70,000 or more per year. Again,

it's important to keep in mind that the job they'll be performing is worth what they're asking. It's an investment you most likely can't afford *not* to make.[5]

1. An inflated pay rate is a small financial setback compared to having a hole blown in the IT system that your company depends on to make a profit.

4. 

See if you can hire a hacker by the job. It may not be necessary to keep a white hat on your IT staff full time. As part of your objectives statement, specify that you're looking for a consultant to spearhead a major project, perhaps an external penetration test or a rewrite of some security software. This will allow you to pay them a one-time retainer rather than a continual salary.

1. The odd consulting job may be perfect for freelance hackers, or those who have recently received their certification.
2. If you're pleased with your cybersecurity expert's performance, you can offer them a chance to work with you again on future projects.

Part 2 of 3:

Tracking Down a Qualified Candidate

1. 

Look for candidates with Certified Ethical Hacker (CEH) certification. The International Council of Electronic Commerce Consultants (EC-Council for short) has responded to the growing demand for ethical hackers by creating a special certification program designed to train them and help them find employment. If the security expert you interview can point to official CEH certification, you can be sure they're the genuine article and not someone who learned their craft in a dark basement.[6]

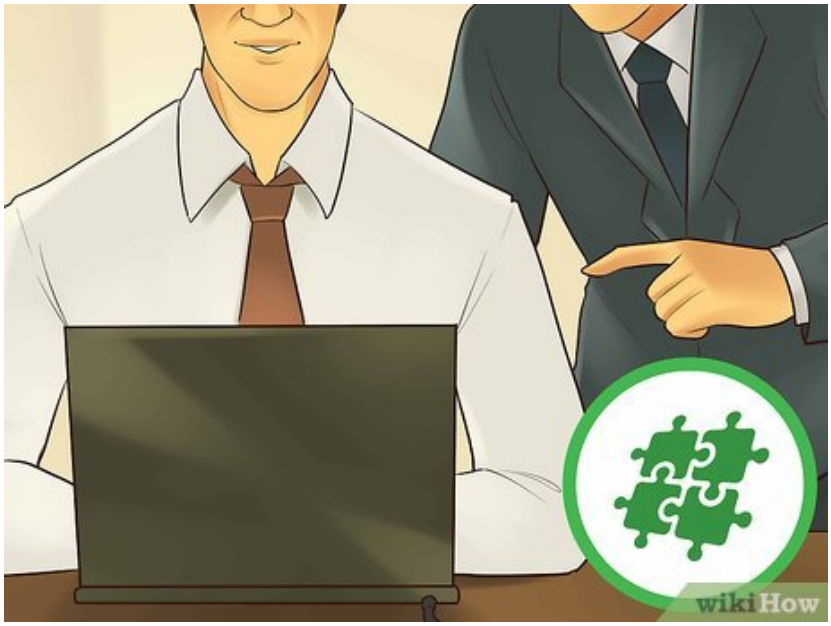
1. While hacking credentials can be difficult thing to verify, your candidates should be held to the same rigorous standards that all other applicants would.
2. Avoid hiring anyone who can't provide proof of CEH certification. Since they don't have a third party to vouch for them, the risks are just too high.

2. 

Browse an online ethical hacker marketplace. Take a look at some of the listings on sites like Hackers List and Neighborhoodhacker.com. Similar to ordinary job search platforms like Monster and Indeed, these sites compile entries from eligible hackers seeking opportunities to apply their skills. This may be

the most intuitive option for employers who are used to a more traditional hiring process.[7]

1. Ethical hacker marketplaces only promote legal, qualified specialists, which means you can sleep easy knowing that your livelihood will be in good hands.

3. 

Host an open hacking competition. One fun solution that employers have started using to attract prospective candidates is to pit competitors against one another in head-to-head hacking simulations. These simulations are modeled after video games, and are designed to put general expertise and fast-thinking decision making abilities to the test. The winner of your competition may just be the one to provide the support you've been looking for.[8]

1. Have your tech team cook up a series of puzzles modeled after common IT systems, or purchase a more sophisticated simulation from a third party developer.[9]
2. Assuming that devising your own simulation is too much labor or expense, you could also try getting in touch with past winners of international competitions like Global Cyberlympics.[10]

4. 

Train a member of your staff to handle your counter-hacking duties. Anyone is free to enroll in the EC-Council program that white hats use to earn their CEH certification. If you'd prefer to keep such a high-profile position in-house, consider putting one of your current IT employees through the course. There, they'll be taught to perform penetration testing techniques that can then be used to probe for leaks.[11]

1. The program is structured as a 5 day hands-on class, with a 4 hour comprehensive exam given on the last day. Attendees must make a score of at least 70% in order to pass.[12]
2. It costs $500 to sit for the exam, along with an additional fee of $100 for students who opt to study on their own.[13]

Part 3 of 3:

Bringing an Ethical Hacker into Your Business

1. 

Conduct a thorough background check. It will be necessary to have your candidates thoroughly investigated before you even think about putting them on your payroll. Send their information off to HR or an outside organization and see what they turn up. Pay particular attention to any past criminal activity, especially those involving online offenses.[14]

1. Any type of criminal behavior that pops up in the results of a background check should be considered a red flag (and probably grounds for disqualification).[15]
2. Trust is key to any working relationship. If you can't trust the person, they don't belong in your company, no matter how experienced they are.

2. 

Interview your candidate in depth. Assuming your prospect successfully passes their background check, the next step in the process is to conduct an interview. Have your IT manager a member of HR sit down with the candidate with a list of questions prepared, such as, "how did you get involved in ethical hacking?", "Have you ever performed any other paid work?", "What sorts of tools do you use to screen for and neutralize threats?" and "give me an example of how defend our system from an external penetration attack."[16]

1. Meet face-to-face, rather than relying on phone or email, so you can get an accurate idea of the applicant's character.
2. If you have any lingering concerns, schedule one or more followup interviews with another member of management team so you can get a second opinion.

3. 

Assign your cybersecurity expert to work closely with your development team. Going forward, your IT team's number one priority should be preventing cyber attacks rather than cleaning up after them.

Through this collaboration, the people creating your company's online content will learn safer coding practices, more exhaustive product testing, and other techniques for outsmarting would-be scammers.[17]

1. Having an ethical hacker there to check each and every new feature may slow down the development process slightly, but the new airtight security features they devise will be worth the delay.[18]

4. 

Inform yourself on how cybersecurity affects your business. Take advantage of your white hat's wealth of knowledge and learn a bit about the types of tactics commonly used by hackers. When you begin to form an understanding of how cyber attacks are planned and carried out, you'll be able to see them coming.[19]

1. Ask your consultant to submit regular, detailed briefings on what they've uncovered. Another way to brush up is to analyze their findings with the help of your IT team.
2. Encourage your hired hacker to explain the measures they're implementing rather than just leaving them to do their thing unquestioned.

5. **Keep a close watch on your hired hacker.** While it's unlikely that they'll attempt anything unscrupulous, it's not outside the realm of possibility. Instruct the other members of your IT team to monitor your security status and look for vulnerabilities that weren't there before. Your mission is to protect your business at all costs. Don't lose sight of the fact that threats can come from the inside as well as the outside.[20]
    1. An unwillingness to explain their exact plans or methods to you may be a warning sign.
    2. If you have reason to suspect that an outsourced specialist is harming your business, don't hesitate to terminate their employment and search for a new one.