Introduction:

Skills within the IT industry are as important as the actual technology. To establish standards and validate skills many IT companies make significant investments in developing and maintaining a professional certification program. Each certification is a valuable asset to both the company and to the IT professionals who ultimately earn the credentials. To protect certification value, IT companies implement practices designed to protect certification tests from compromise and to provide overall test security.

IT certification programs have become increasingly focused on test security issues, and have placed particular attention on activities the general public commonly refers to as ‘Cheating’.

Most individuals avoid such deception and achieve certification honestly. They develop the necessary skills & knowledge for personal growth and professional development. These individuals invest the necessary time to prepare appropriately and to earn the credential. This honest majority is deserving of the recognition that is awarded to the certified IT professional.

However, there is a subset of individuals who lack the personal responsibility to achieve a certified status based on their own accomplishments. They are the minority who resort to cheating on tests. These individuals attempt to deceive employers and peers by misrepresenting themselves as “certified.” Others resort to stealing questions from these assessments, thus not demonstrating their skills but rather taking illegitimate shortcuts to earn these certifications. These unlawful individuals violate the trust of the public, clients, colleagues, and the certification community. These are people who, through means of deception, steal value from professional certification.

Professional certification programs associated with the IT Certification Council (ITCC), a council of IT industry leaders focused on promoting IT certifications, recognize the negative effects of cheating on the industry. As a result, and on behalf of the honest majority, certification programs are working together to protect the integrity of IT certification and re-establish value previously lost to deception and misrepresentation.

The ITCC provides a joint framework for collaboration amongst the membership. As a team, the ITCC has engaged in a variety of projects which involve securing certifications. Their collaborative activities are now specifically focused on methods to combat cheating. As this positive momentum continues to grow, a few key points are becoming increasingly clear:

- IT professional certification programs, across the industry, are taking action against cheaters
  - Targeted actions taken by the certification programs have proven to be successful
  - Thousands of individuals have been identified and have had their credentials revoked
  - Various different processes are in place to address cheating
  - Continued focus on certification test security initiatives has resulted in ongoing process improvements

The purpose of this white paper is to outline the importance of honest test taking, the risks one takes when attempting to cheat and the measures being taken by groups (such as the ITCC) to counter fraudulent test taking. As a current and/or future IT certification candidate, it is in your best interest to take this information to heart as you begin (or continue) your efforts to better yourself and your career through one of the many available IT certification programs.
NITT: Basic Cheating 101:

What is NITT? NITT (Non-Independent Test Taking) is the type of cheating most commonly discussed amongst test providers. NITT is widely defined as test-taking with an aid.

Dishonesty takes several different forms in the arena of certification testing. Each can be uniquely identified and addressed. Some of these distinct methods can also be categorized as NITT.

NITT covers a broad range of activites that occur when a test taker chooses not to test on his or her own. Instead, they receive some sort of inappropriate assistance. Inappropriate assistance can be provided by other individuals, technology, or physical materials. Examples include sharing of test questions, obtaining copies of the certification exam, using guides during testing that are kept hidden from proctors, etc. As a result of assistance, the answers provided by the test taker during the exam are not necessarily their own independent responses. Therefore, these test results are not a valid assessment of the knowledge and skills of the person who registered to take the test. In turn, the test results are meaningless.

Taken as a collective group, NITT is the most prevalent form of cheating. As such, each component of NITT is, individually, a subject of much scrutiny. With the implementation of new test security initiatives, professional certification programs are beginning to make significant strides to identify individuals who participate in NITT.

There is a recent initiative that has generated a great deal of interest. Its purpose is to identify specific test takers who acquired the actual certification exam, prior to taking the test. (Unfortunately, some people obtain a stolen copy of the certification exam to “study” [memorize] before testing). The initiative is launching in a staged roll-out. In the early stages, the methodology has already proven to be very effective in the identification of those who participate in this form of cheating.

Penalties for the identified individuals are usually significant. Typically, the associated certification is revoked (if awarded). Additionally, the individual is banned from testing for an extended period of time.

All deceptive activities are taken seriously. In addition to NITT, there are several other forms of certification cheating. Whenever a form of cheating is detected, the applicable certification program will respond swiftly by issuing a penalty. Therefore, it is of utmost importance to always be cognizant that your study materials are materials approved or provided by the issuing IT certification program.

Common Forms of Cheating Within IT Certification:

The elements of this problem are varied and significant. Some of the recurring challenges met by most IT certification programs are as follows:

• **Stealing IP** - All exam content, including the items, options, and correct responses, is the intellectual property (or IP) of the certifying agency. There are a growing number of individuals who will go to extraordinary measures to obtain actual exam content. There is high demand from intentional cheaters as well as from potentially uniformed candidates who are searching for study resources. IT certification programs and their test delivery providers take standardized measures to secure the test content. Test content is expensive to produce and very difficult to replace. Whether exam stealers (pirates) infiltrate the communications between the certifying agency and its vendor,
take a test to solely memorize the content, or take any other step to intercept the test content, pirates are at the center of the security problems.

• **Sharing questions or answers with others** - Some test takers discuss the results of their exams with fellow candidates. It is natural for most to have experienced this and to want to discover the answer or discuss shared challenges, in an effort to understand the content of the exam. These discussions can occur in person, through email, or through online community forums and chat rooms. However innocent these discussions may seem, all IT certification programs have Nondisclosure Agreements (NDA’s) and candidate agreements in place that specifically prohibit sharing information from a test. The reason this sharing is prohibited is because candidates end up working together to figure out an answer—a dynamic referred to as “collusion.” In short, certification programs wish to certify individuals based on their own knowledge and skills and not on a “collective knowledge” gathered from discussions. In addition to collusion, discussing items from a test, especially in public forums such as online spaces, may also pre-expose other candidates who have not already taken the test. Both collusion and pre-exposure inhibit a certifying agency from doing the job of certifying an individual on their independent knowledge and skills. By giving help on a test item or teaching others the content found on an exam, candidates are essentially enabling someone who may or may not meet the qualifications of the certification to pass the test.

• **Cheating during the test** - Cheating during a test has become a sophisticated strategy that no longer is limited to bringing cheat sheets and unauthorized notes into the testing environment or copying answers off another candidate’s test. In this digital age, candidates have smartphones and other mobile technology to aid them in cheating. This type of cheating can be detected with data forensics and is often backed-up with video or eyewitness evidence. Candidates who are discovered cheating during a test can be subjected to decertification and can be banned from testing with a specific program or testing center again.

• **Taking a test for another** - Proxy test taking is when one individual takes a test on another individual’s behalf. This behavior is considered test fraud because the results of the test are not those of the person seeking certification. Those who commit this type of fraud risk their identities and their professional integrity. They pay large sums of money to individuals they have likely never met and provide them with intimate details of their personal backgrounds, up to and including copies of their government-issued ID. IT certification programs have gone to great lengths to detect this type of fraud, including requiring photos on score reports, digital signatures and more. Candidates should also be aware that entering into transactions with organizations that engage in this unethical business method is risky and could result in identity theft.

• **Falsifying scores or the ownership of a credential or certification** - A few candidates will go to any length to obtain certifications, including falsifying their certifications by altering their score reports or producing other false “proof.” Again, this is test fraud and can easily be tracked down by the IT certification program.

• **Downloading or Using Brain Dump Content for Test Preparation** - While innocently preparing for certification, candidates may have discovered websites that offer “study guides” or practice materials that come with a guarantee of a passing score. In most cases, these companies boast the effectiveness of their product and will cite validation of the content by actual instructors. These websites are called brain dumps. The phrase “brain dump” refers to a collection of confidential information relating to examinations, which is obtained by examinees who memorize, or electronically capture the content, then “dump” (or record) the information after the examination. Brain dumps are also a way to refer to collections of exam items that have been stolen from high-stakes certification
exams. While many of these companies and sites blatantly detail their illegal source of the testing material, others do not. Either way, the content is stolen IP. Candidates should watch for basic signs of brain dumps, which include lures like money-back guarantees, 100% pass rates, and other too-good-to-be-true promises. IT candidates should be careful of what companies they use to find additional preparation resources. To be sure of the validity of a site, you should be in touch with your IT certification program. Often, the IT certification program will have recommended sponsored sites that can be trusted. If it sounds too good to be true, that is a good sign for a test taker to avoid the site. Most importantly, candidates should always be mindful that obtaining a copy of a certification exam is cheating. When caught, the consequences can be severe.

• Not understanding or following the terms of an NDA - IT organizations require candidates to agree to an NDA before they can take an exam. This agreement usually includes the specifics of what is expected of candidates and which types of study resources are prohibited. Candidates can familiarize themselves with the terms of an NDA by visiting the IT certification program’s website and downloading the terms in advance.

Anytime cheating is suspect, it can cause doubt about the value of the hard-earned certification. Potential employers often use certifications to identify those candidates who have the minimum skills, knowledge, and potential ability. Likewise, those with certifications tend to earn higher salaries and are valued highly. As candidates knowingly or unknowingly subvert the certification programs, as in the examples listed above, they run the risk of diminishing the value of the very credentials they seek. In turn these candidates negatively impact the importance of the very certification they are attempting to falsely acquire, thus diminishing the likelihood of a raise in salary.

What Types of Actions are IT Companies Taking?:

Multiple tactics are needed to combat cheating. You will find that IT companies utilize various methods to address the issue. These actions include:

• Analyzing all test results to identify candidate participation in NITT
  o Perform data forensics and other types of statistical analysis
  o Examine testing patterns
• Banning a candidate from testing for a defined period of time
  o As an example, perhaps disallow any testing for a period of six months
  o In some cases the testing restriction can be for life
• Revoking certification(s) and the associated certified title
• Taking legal action to remove content from brain dump sites and blogs
• Frequently refreshing exams so brain dump sites become outdated and inaccurate
• Closing testing centers:
  o With questionable testing results
  o Do not comply with security standards and candidate identification
• Publishing blogs to educate test-takers about proper study and exam behavior
• Monitoring social media sites and forums for inappropriate behavior
• Implementing tough ID standards/processes to combat proxy testing entities
• Requesting payment processor companies to stop doing business with brain dumps

IT companies are finding that a mix of tactics is most effective. They are also finding that more is needed to be truly successful.
Communication is Key to Success:

The objective for IT professional certification is to reduce the number of security incidents related to the various types of fraud and deception. There are three specific components required to achieve this objective:

1) Identify the individuals engaged in the act
2) Enforce appropriate penalties for the violation with consequences considered to be of significance to certification candidates (and other interested parties)
3) Generate awareness of the actions taken to address this type of inappropriate behavior
   - Communicate that individual cheaters can be (and are) identified
   - Deliver the message related to the strict enforcement of penalties
4) Establish security standards and policies and communicate these to stakeholders

In the fight against cheating, the necessity to identify and penalize cheaters is rather obvious. However, not so obvious, but equally (if not more) important is the need to communicate these actions. The impact on cheating will be isolated and minimal, without widespread awareness of the activities in place to combat cheating. Communication is needed to drive awareness.

With successful execution of the four components listed above, a reputation for being tough on cheating can be firmly established.

Simultaneously, messaging is needed to generate a higher level of awareness and an understanding of the underlying purpose for these actions. The ultimate goal of test security is to protect the integrity of IT professional certification and increase value. To this end, messaging is necessary to:

- **Share communications with the IT certification community** - The security initiatives are designed to protect the integrity and value of certifications honestly achieved by investing time & effort to develop the necessary knowledge & skills. Integrity is maintained when individuals without validated skills are identified and the appropriate, corrective action is taken so these individuals are not allowed to misrepresent that certification. In short, this corrective action upholds the certification value of IT professionals who properly prepare and who earn the recognition of their certified skills.

- **Advise IT professionals** - Information regarding the benefits of certification test security is also being conveyed to employers, highlighting key points; such as:
  1) The industry is taking action to address fraudulent activities related to IT professional certification.
  2) One element of these test security initiatives is to revoke the certification credentials from individuals who are found to be participants in NITT or have been found to be participants in any type of activity identified as cheating.
  3) Employers can have an increased level of confidence the skills of certified IT professionals have been appropriately validated by the certifying agency.
  4) As a result, certification can be even more valuable when evaluating employees or in differentiating potential candidates during the hiring process

- **Educate test-takers** - Candidates should be aware of testing policies, practices and requirements of the IT certification programs. As a general rule, testing policies and requirements listed on the IT certification program’s web pages. It is very important for each test-taker to have a
clear understanding of the rules they will be held accountable for following. Everyone should carefully review the testing policies as a prerequisite to test preparation. The recommended methods to prepare for tests, including authorized study materials, are also typically listed on the IT certification program’s web site. Following the vendor’s recommendations for test prep is always the best approach, and the recommended material can be used with 100% confidence. By promoting these credible and informative messages, many more candidates will be driven to learn about testing requirements and the appropriate methods for test preparation.

**Summary:**

IT professionals are increasingly looking to certifications to demonstrate their knowledge, skills, and competency to potential and current employers. However, an increasing percentage are trying to achieve certification through dishonest means – namely, cheating. By cheating, IT professionals diminish the value of these certifications to employers, customers, and the certificants themselves, while damaging the ethical standards upheld in the IT industry. This IT Certification Council (ITCC) white paper walks IT professionals through the ways cheating commonly occurs, how certification companies are identifying cheating, and the consequences of these actions when recognized and caught. By understanding cheating in IT certifications, IT professionals can help educate each other and ensure that their hard earned certifications maintain a high level of value around the industry.

**Learn More:**

You can learn more about the importance of securing certifications at ITCC’s website. Visit the website for other whitepapers regarding the importance of IT certification and honest test taking.

- ITCC’s Website
- ITCC’s White Paper Library