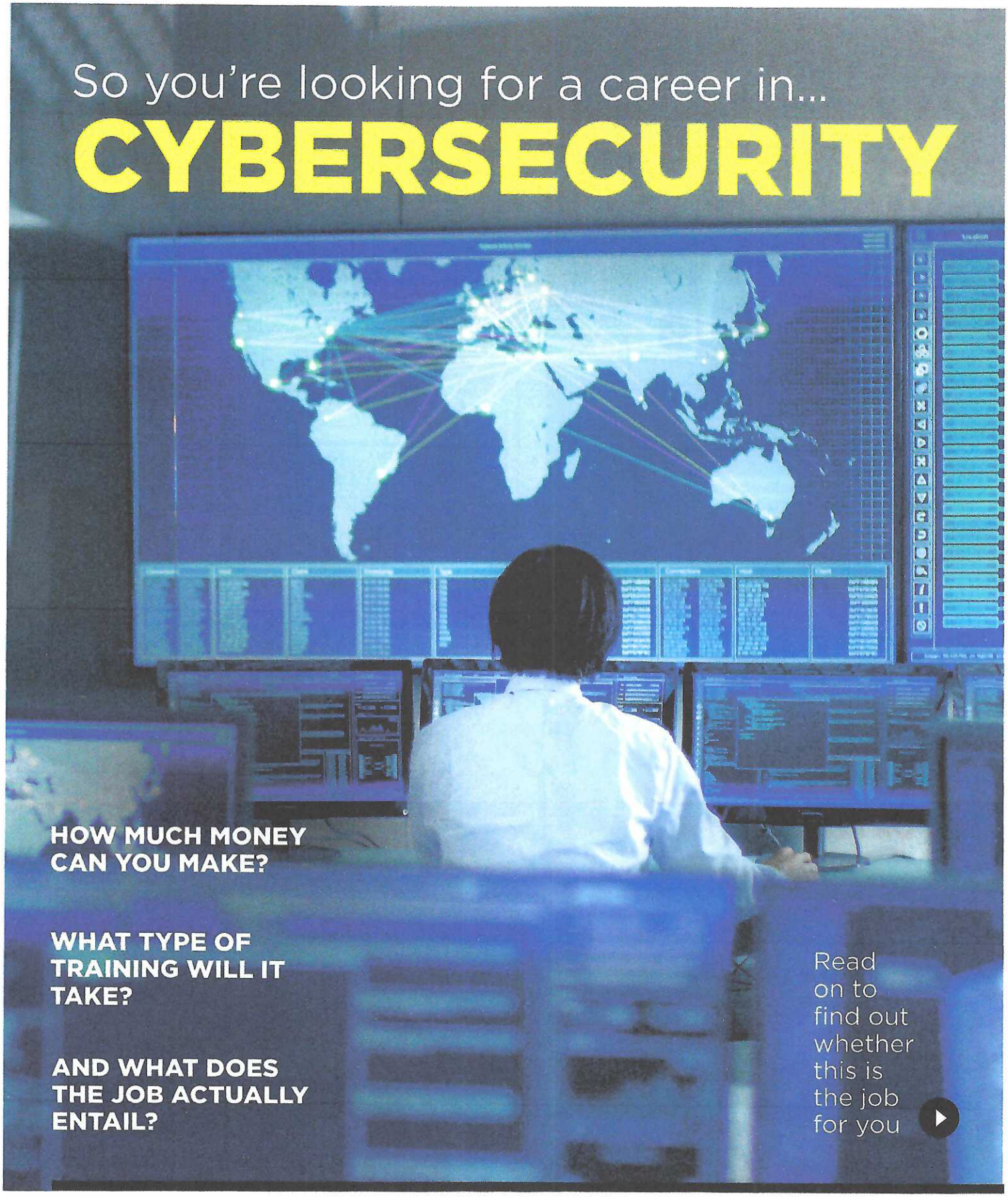
So you're looking for a career in...

CYBERSECURITY



HOW MUCH MONEY CAN YOU MAKE?

WHAT TYPE OF TRAINING WILL IT TAKE?

AND WHAT DOES THE JOB ACTUALLY ENTAIL?

Read on to find out whether this is the job for you

WHAT IS CYBERSECURITY?

Cybersecurity is the practice of protecting computer networks, systems, servers, and programs from malicious digital attacks. As more of the institutions that support our daily lives rely on computer systems to function, the need to protect these systems from attack becomes stronger than ever. As such, cybersecurity is one of the hottest computer-related fields today.

WHAT CAN I EXPECT TO EARN?

Salaries vary based on the type of work, level of experience, and location. Some median wages:

IT Security Specialist:
$97,000
Information Security Analyst:
$76,000
Security Engineer:
$102,000
Intelligence Analyst:
$65,000
Security Specialist:
$97,000
Security Consultant:
$87,500

WHAT WILL I BE DOING ALL DAY?

As a rapidly growing field, there are a variety of job paths you can choose within cybersecurity. Here are some of the most popular:

Chief Information Security Officer (CISO). This person oversees the general operations of a company's IT security division. The CISO works with the company's managers to determine the company's cybersecurity needs, and assembles a security staff to put the system in place and manage it.

Information Security Analyst. This person plans and executes programs to protect an organization's computer systems and networks. This includes installing software and also designing methods for data recovery following attacks.

Penetration Tester. This person is essentially an authorized hacker, who proactively attempts to break through a computer system's security in order to identify the areas of vulnerability.

Forensic Computer Analyst. This person is known as the detective of the cyber security world, whose job is to review computer data for evidence following a security breach.

IT Security Engineer. This person uses a specialized engineering approach to design security systems. Security engineers are often involved in systems maintenance and developing methods to track security incidents.

DO I HAVE THE PERSONALITY FOR IT?

These are some of the traits that make for a good cybersecurity professional: self-disciplined, driven, curious, out-of-the-box thinker, intelligent, and focused. The nature of the profession also demands a high-level of personal integrity and discretion.

WHAT SCHOOLING DO I NEED?

While it looks good to prospective employers to come in with a degree, and there are several good graduate programs for a *frum* clientele in cybersecurity, what matters most in this field is field-specific training and passing certification tests. Before specializing in cybersecurity, you need a thorough grounding in IT (information technology) — in how computer networks work and in programming skills. Knowledge of Linux and Windows operating systems and three or four basic programming languages (PowerShell, Python, Bash) are a must. Once you've mastered this and acquired several years' experience in the IT field, you can then go on to train for and take one of the specialized cybersecurity certification exams.

Coming up soon in future installments of Job Search: **Catering** and **Accounting.** If you work in these fields and would like to share your experience, please email info@mishpacha.com

TALES FROM THE TRENCHES

THREE CYBERSECURITY PROFESSIONALS DESCRIBE THE HIGHLIGHTS AND THE CHALLENGES

MENACHEM ROTHBART, LAKEWOOD, NJ

Lead Penetration Tester at Nettitude Inc., Manhattan branch
Years in the field: 8 (3.5 in current position)
Training: Offensive Security

A TYPICAL DAY AT WORK LOOKS LIKE...

After answering emails and finalizing reports from previous engagements, I get started on the day's testing. Be it web apps, networks, mobile apps, or more, I fire up my tools and get started on hacking some complex client applications in order to find flaws before the hackers do. During the course of the day, I'll be sought out by account managers or fellow testers for advice. The workflow itself is pretty fluid, given that there's a lot of thinking in this work. It's not a checklist to be followed. There can be a lot of downtime, and then suddenly inspiration strikes and there's a period of frantic work. I like to get the usual easy vulnerabilities out of the way early in the day so that I can focus on the more exciting exploits that come from a really cool hack. When we do find something fun, we can be drawn down the rabbit hole of multi-part exploitation, and there are times when a single vulnerability can lead to several days of work, creating an impactful attack chain to show just how powerful a flaw can be.

I CHOSE THE FIELD OF CYBERSECURITY BECAUSE...

I've always loved computers. I began programming when I was in fifth grade and worked on my first professional project when I was in tenth grade. As I grew older, I discovered that it wasn't the programming that I enjoyed, it was making computers do what I wanted them to do. At that point, it was a simple lateral movement to security. My natural thinking tends toward rule-breaking, and hacking was a very good way of channeling this in a constructive manner. I got into the field just as it was becoming big, and being paid to break rules and hack things is a dream come true.

WHAT I LOVE MOST ABOUT THE FIELD IS...

The stories I get to tell. Whether it's about the time I was able to steal classified information from a bank and gain access to all the account, the terrorist watchlist, and the SWIFT transaction system, the time I cracked a bunch of passwords to find that they were created by *frum* Jews ("TalmudTorah05," "Kosher07212017"), or the various social engineering hacks via email I was able to pull off, each engagement is its own cool story. Sometimes I laugh when I tell the story of how I walked around a massive institution with a camera and took pictures of passwords and documents without being challenged, and sometimes I have a bit of remorse when I tell the story of how I stole a password and hacked a massive international company with it. Sitting around a lunch table with other penetration testers is a lot of fun, as we trade our war stories — and it's great learning too, as we learn from each other's techniques.

WHAT I FIND MOST CHALLENGING ABOUT THE FIELD IS...

Honestly, very little. My company is extremely respectful of me and my religious needs. I never have to go in to work on Fridays or Erev Yom Tov, they've never given me a problem about taking off of work, and they even let me work from home during Chanukah. I'm extremely lucky to be where I am.

My biggest challenge is making sure the report I create at the end of each engagement has proper remediation advice for the client, is in an easily actionable format, and makes them feel they got their money's worth. With some engagements, this can be difficult, and I put in a lot of effort into my reporting to make sure it's up to par.

MY ADVICE FOR PEOPLE STARTING OUT IS...

Keep reading and learning. Don't get discouraged by the sheer volume of information you need to know. There isn't a hacker in the world who doesn't learn something new every single day. Reading up on the newest literature is great — but the best place to learn is to tinker around yourself with the plethora of free tools that exist online. Always seeking to know more is the single defining trait of a hacker.

SENDER SCHWARTZ, RAMAT BEIT SHEMESH
Ethical Hacker, owner of PC Works computer servicing
Years in the field: 2 (25 years in the computer field)
Training: Campus Strauss — Lomda Institute

A TYPICAL DAY AT WORK LOOKS LIKE...

My cybersecurity day begins with reconnaissance. First, I get as much background as possible about the client, whether it's a smart home, office, or "secure" environment. I visit the location in person to see firsthand the physical makeup and what kind of security systems are currently in place. Next comes researching the physical systems to determine their vulnerabilities and formulate possible approaches to infiltrate them. I'm actually in the middle of a project now, trying to break into a smart house. I found two holes in the system, where I was able to trick the computer into allowing me access with full control over the entire house.

I CHOSE THE FIELD OF CYBER SECURITY BECAUSE...

I've run my own computer servicing business for 25 years, in which my team and I build, design, and maintain computer networks for home users and small businesses. During these past 25 years, technology has evolved at an extremely rapid pace, making computers and computer networks increasingly vulnerable. Everyone knows someone whose email account was hacked, credit card number made public, or who was spied on through their computer webcam or microphone.

Many believe that hackers are primarily an issue for big corporations, but your average online intruder is actually much more interested in gaining access to an individual's computer — because the police will not allocate major resources to the individual the way they would for a corporation. Your average retiree who regularly monitors his stocks and retirement accounts is unaware of the potential pitfalls on his desktop. And we're much more vulnerable today with smartphones. People just tap without thinking. So I choose to focus my work on the personal user and small business rather than large corporations, because this is where I can best use my strengths to help the most people.

WHAT I LOVE MOST ABOUT THE FIELD IS...

It's never boring — things change on a daily basis. After all of the hard work in gaining access to a "secure" system, it's rewarding to find someone on the other side who watches what I'm doing and tries to stop me — it's like we're playing chess. The clients are the winners in every game, because when I'm done, their systems are safe.

WHAT I FIND MOST CHALLENGING ABOUT THE FIELD IS...

Since new vulnerabilities are discovered daily, you must constantly keep up-to-date, which is very time-consuming.

MY ADVICE FOR PEOPLE STARTING OUT IS...

Don't get discouraged. You'll experience lots of penetration attempts that don't work out. I've learned more from those failed attempts than from my successes — they have helped me grow my expertise and ability to assist others in protecting their assets.

LEAH FREIMAN, SPRING VALLEY, NY
CEO, ITCon Inc.
Years in the field: 12

A TYPICAL DAY AT WORK LOOKS LIKE...

I run a company, together with my husband, that provides IT-managed services and IT cybersecurity services to businesses. Our average client has between 150–600 employees. A large part of my job is education — teaching clients about cybersecurity, why we need to be so careful nowadays, and raising awareness about compliance with state laws. If companies have a breach in their system, no matter how large or small the company is, they are in major trouble. Sadly, most reach out to us only after the breach. We like to get the clients before they have a problem. By doing an assessment on their system and telling them where their vulnerabilities are, we're able to protect and prevent havoc. We produced a documentary called *Cybercrime* on that topic and we also have a full free end user training program to help people understand the importance of cybersecurity and how cybercrime can affect them.

Cybercrime is the fastest growing industry in the world, and there's so much money to be made so easily, because it's all done anonymously. Also, most companies are not protecting themselves, making them low-hanging fruit and very easy prey — 99.9% of hacks are preventable! For every security product that's out there, there's a hacker that knows how to circumvent it. So, my job is to make sure my clients are up-to-date with their protection — while also ensuring that they aren't oversubscribed. It's a fine line between protection and user-friendly.

I CHOSE THE FIELD OF CYBERSECURITY BECAUSE...

I actually started out in a different field altogether, as a mortgage broker. When the real-estate market crashed in 2008, I needed to find a new job. My husband had gotten certified in IT, and we decided to open a business together, with him doing the technical part of the work and me running the business side. After several years of providing computer system repair services, we moved over into a proactive business model, by setting up systems with the optimal security. Our clients have monthly service contracts with us, and we also manage in-house IT teams. Baruch Hashem, our company has grown exponentially over the past few years, and we now have a full-time network operation center (NOC) and security operations center (SOC).

AS A WOMAN IN THE FIELD, I DON'T NECESSARILY FIND IT TO BE MALE-DOMINANT, AND YET...

The field definitely tends to attract more men, and I'd say there are certain qualities of a cybersecurity professional that tend to be associated more with men, but there are definitely women in the field as well. Ultimately, this is a service business — it's about communicating with and helping the customer, and those are the kinds of skills women are great at.

However, this is a 24/7 business. Since we're protecting our clients in real time, we need to be available for our clients around the clock, whenever there's a problem, and one of the first questions I ask a potential hire is whether I can wake him up in the middle of the night. So this isn't the type of job that many mothers can do.

WHAT I LOVE MOST ABOUT THE FIELD IS...

Helping people. I love knowing that I have the tools, processes, and procedures to be the "savior of the day" when an emergency occurs. Even more so, when we get security alerts and proactively prevent a hacker from accessing a company, I think of all the jobs and money that is saved, of all the headaches and pain this company would be in had we not implemented the right security tools. The satisfaction is tremendous.

WHAT I FIND MOST CHALLENGING ABOUT THE FIELD IS...

Educating the end users about what we do. I find that the employees in our clients' companies — the people who are actually using the systems we set up, the secretaries, the accounting department — will call us complaining that what we set up isn't working. But in actuality, usually it's because they simply haven't been trained in how it works.

Also, you'll have the occasional new CFO who comes in and decides he's going to save the company money by bringing in his brother-in-law who can do it cheaper. CFOs and managers have to prove themselves. Saving the company money makes them look very good, but they don't necessarily understand what we do. Ultimately, the two clients that did leave us for this reason came back within the year.

MY ADVICE FOR PEOPLE STARTING OUT IS...

Start from the bottom, and get lots of experience. Cybersecurity is a great field, and there are so many niches you can branch out into, but you can't become a heart specialist without going to medical school — you need a thorough grounding in IT first. Our clients don't know anything about this field, so they're trusting us to do it right, and if we make a mistake, we can mess people up really badly. Be transparent with clients about what you're doing and what tools you're using.