FILE UNDER:
Cybersecurity » Phishing

A special interview with

JASON GOLDFARB

macOS Security and Mobility Specialist

TECHNOLOGY REVEALED LLC

In decades past, cybercrimes generally amounted to pranks by geeks and nerds having a good time with technology.

But these days, cybercrimes are catastrophic and costly — to individuals, businesses, and even nations. And almost all of them begin by taking advantage of human vulnerabilities.

The issue has become so important that we asked our communications agency, The Creative Offices (TCO), to discuss the matter with our macOS Security Specialist, Jason Goldfarb.

Jason has been our senior consulting engineer for nearly 20 years, and holds multiple certifications from Apple, CWNP, and Google.

TCO: Let's start with the basics: What's phishing?

Jason: Phishing is a technique that hackers use to try to steal information from end users; information that can be used against them.

In real-world fishing, you bait a hook with a worm or lure or something else that will get a fish to do what you want: Bite.

In the cyber-world, hackers use fear and psychology to bait people into doing what they want: Pay.

A hacker might send an email saying, "Hey, I've been watching you and I know your pornography preferences. I'm going to send a copy to everyone in your address book unless you send me money."

Or a hacker might write, "Hey, this is your bank, we've had some cybersecurity issues on your account and we want you to click this link to log in and make sure everything is okay."

Then the end user thinks, "Yikes, I've got problems on my bank account." So he or she clicks the link; and it takes them to a web page that looks exactly like their bank's page.

The user puts in thier credentials, but instead of logging into the real banking website, they just delivered thier banking account information to hackers.

At this point, they're vulnerable to all sorts of identity theft and everything else that goes along with it.

So the bait part is the email. It's the social engineering part that makes people want to click the link. The hook and reel part is where they trick you into continuing, thinking that you're doing something legitimate.

TCO: After putting in a username and password into one of these phony websites, are users notified somehow that an attack has occurred?

Is there some hint or trigger that they didn't submit their info to a genuine site?

Or is the process so transparent that it ends with users logged in and looking at real account data?

Jason: There's a lot of really interesting things that go on there, but typically what they do is redirect users to another page that will say something like "Due to some technical difficulty, our site is down."

Or they might redirect users to the bank's real login page, and at that point users are just prompted to authenticate a second time.

A lot of people are like, "Well that's kind of weird, but I'll log in again."

> "Avoiding this type of social engineering is very simple.
>
> If you get an email from your bank, from Google, from anybody that's asking you to click a link to do anything, **go to the site directly** and then login."

TCO: So that's something the average user can latch onto. If they have to put in a password again, maybe it's time to worry and think, "Hey, something fishy is going on here, and I need to be worried."

Jason: Here's a new one that I just read about the other day. People will get a prompt in an email to login to their Google account. And because they're told there's some type of security issue, they'll click the link.

It'll take them to a malicious page that looks exactly like Google's login. Every single thing is exactly the same.

They fill in their credentials; and because they have two-factor authentication (2FA) turned on at Google, they think they're secure, right?

Wrong.

What happens is, the back end of the hacker's website captures the user's login and password, and sends it to Google. Google then sends them a 2FA code via text message, voice call, or email.

The hacker's program then brings up a window that looks like Google's 2FA response page. The end user types the code they received into the phony page. The hacker captures the code, and then inserts it into the real Google page. Then they have full access to the user's account.

TCO: So what can users do differently?

Jason: If you get an email from your bank, from

Google, from anybody that's asking you to click a link to do anything, go to the site directly and then login. That's the best way to thwart this type of social engineering.

So if your bank sends you something like, "Please click this link to continue logging into your account," don't click. That's all: Do not click.

Instead, go to your bank's website by typing the URL by hand, login, and then see if they've really sent you a message.

That is the easiest way around it.

And that's what we really need to train the end users to do. The task is difficult, however, because people like to click links.

Clicking is fast, clicking is easy, but I can't tell you how many people invite problems by clicking links — in emails from banks and shops, in popup windows requesting updates, and so on.

That's how bad stuff happens.

I tell people, if anything ever pops up on your screen asking to update a program, go to the application, and look for an update menu item.

If it's Adobe Flash, you can go to your system preferences, click on the Flash Player icon, and check your update status. If you're up to date, then you don't need to do anything. And if you're not up to date, you can update it right from there.

Training the end user on how to recognize things that might be malicious, even if they're really hard to discern — that's the key.

It's less about what things look like and more about the process. Being asked to click something to authenticate, to provide personal information, or to initiate an update, *that's the red flag*. And if you see that, it's best to complete the task manually; because only then will you know it's valid.

TCO: Okay. How big of a problem is this really? It seems to me that a lot of this would affect consumer users more often than businesses.

Businesses have firewalls and policies and tools of all sorts that work to preserve the integrity of their networks. What's really the danger for them?

Jason: Businesses are at tremendous risk.

While enterprises have firewalls, proxies, anti-virus filters, and have anti-malware technologies on their networks, keep in mind that all these things can cost tens-of-thousands or hundreds-of-thousands of dollars and require a cadre of IT people to maintain. These are resources not available to the average small business.

Moreover, all businesses still have human users that are vulnerable. So while enterprises are protected to a greater degree than small and mid-size businesses, they still need to worry.

Every employee who is in front of a computer is a risk. A lot of people are now working in an environment where users have hot seats or participate in a just-in-time workforce. IT will give a user a laptop and they work from home two days a week and then work three days in the office.

Well, they take their laptop, go to a coffee shop because they're still working. Everybody's mobile now, and everybody's always working.

Coffee shops are a rat's nest of garbage when it

comes to the Wifi and security. There's basically no protection at all.

Jason: I'll tell you a story: Unknown to anybody at the time, a Company's business partner was phished at some point in the past and their email account compromised.

Fast forward a bit, now a business deal was being done and a lot of emails with banking details were moving back and forth.

The hacker who had stolen the account data had been lurking, *waiting*, watching all of the email traffic back and forth in real time.

The project was about to close, and an email with account information was sent so the parties could finalize the deal.

Suddenly, another email came saying there was a mistake in the account number, and the real number would be coming in a new email.

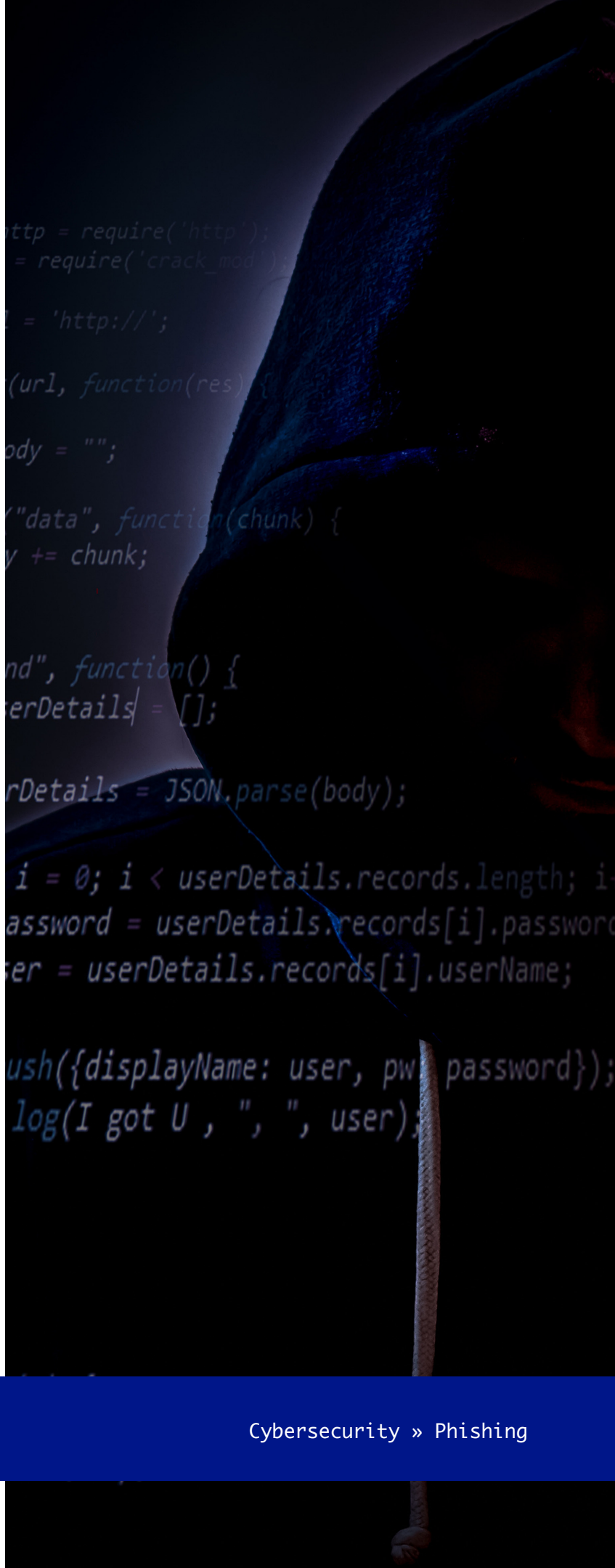
That email came, the account number was indeed different (and bogus) and the deal went through, but the money went to the hacker, not the partner.

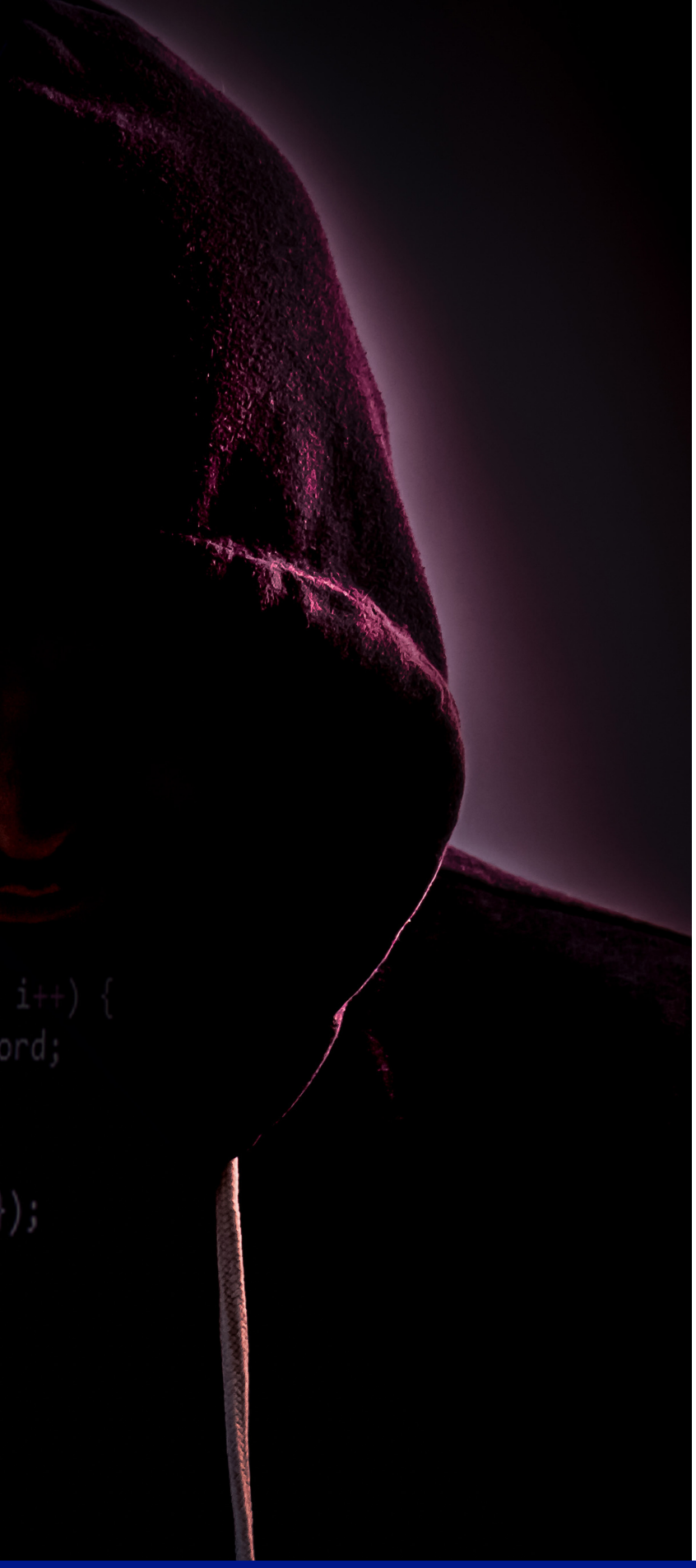
TCO: Was any of that money recoverable?

Jason: Because they found out about it soon after it happened, they got the FBI involved and were able to trace and recover the money quickly.

It's important to remember that phishing doesn't always lead to an immediate catch. You might get phished and nothing happens for a few years.

But they're maintaining the access and somebody's watching. And then all of a sudden there's an opportunity and they jump on it.





I had a client the other day who called up and said, “I got an email that said somebody’s watching my webcam and he knew my name, knew my address, and even knew my passwords. I’ve been hacked, what do I do?”

But the client wasn’t hacked.

The most likely scenario is that there was a data breach at another company. Big box stores, major online retailers, there’s been thousands of data breaches and millions of people’s information has been released. It happens all the time, and that’s where some hackers get information like that.

Then they use it to gain credibility in their phishing schemes. They email you and say, “I know your name, I know your address, and I know your password.”

Most people are bad about using multiple passwords on the different sites. They use the same password everywhere. So when an email with that password is received, they panic because it seems legitimate.

But it’s all social engineering, fearmongering, and guesswork.

Jason: Here’s a little puzzle: Somebody sends you an email before an NFL game, and in it was the winning pick for that game that night. You get one of these before every single game and each one was a winner. Now you get an email before the Super Bowl saying if you give the sender $50,000 they’ll send you the winning pick. Would you do it?

TCO: Who wouldn’t?

Jason: Okay, well that’s the question. This is how phishing began.

Let's simplify the math and say the hacker sends out 10,000 emails, and he breaks the teams up so that half the people get one team and half the people get the other team.

The first game of the season, he has 5000 people he sent the right pick to.

Second game, he cuts that list in half again. Half get the losing team, half get the winning team.

Now 2500 people get the winning team.

As you go down the line, eventually you get five or 10 people who you have been the correct pick every single time. There's no magic behind it, it's just a numbers game.

So those people are thinking, "every single time the game has been played this guy's given me the right answer, so I'm going to trust him and pay the $50,000 because I'm going to bet $200,000 on the game."

And it's a 50/50 shot whether they're going to get the real answer or not, as was every other one.

Way back when, hackers cast a wide net, put vague information into an email, and bet that some people were going to bite.

To avoid these kind of scams, stay savvy, understand where bad actors are playing, and trying to stay out of that pool, so to speak.

TCO: What does the cleanup from all of this typically run, in terms of time or in terms of money?

Obviously somebody who loses their identity or has an outright theft in the way that you described with real money stolen, those are pretty easy numbers to quantify.

But in terms of the average business that's attacked, how long does it take to clean up their network so that this doesn't happen again? How long does it take them to recover from that?

And do they have to disclose to their customers that there's been a successful hack?

Jason: As far as I know, the only people who are required to disclose are in regulated industries.

By that I mean, they're also the ones who are required to remediate.

Let's look at a company like Technology Revealed, for example. We're not subject to regulation like the health or finance industries.

If somebody hacked into our Quickbooks file and paid themselves $50,000 out of our funds,

we'd be under no obligation to tell our clients that.

Maybe what we do to fix it is to change our passwords and up the security on our router. So the cost of recovery in such a case is pretty low.

But we're an IT company.

To bring in outside help can run a few thousand to a tens-of-thousands of dollars, depending

on the size of the network. To clean up breached systems, it can can take a couple days to a couple weeks to harden security, retrain users, and so on after an attack.

But, the *major* costs come from cryptolocker viruses. We haven't talked about that much because it doesn't really affect us yet on the Mac side. but cryptolockers are direct ransomware. These kinds of breaches literally lock (encrypt) the data on a user's or a company's computers and servers unless and until a ransom is paid.

Ransomware has shut down hospitals, air traffic control, radio stations, even the city of Atlanta for a time. In some cases there is no choice but to shut down because there is no access to computer systems during an attack.

If there is no disaster and remediation plan, the only solution may be to pay up and pray that the bad actor actually does what they say they're going to do and unlock your files.

The drawback is that now you've been targeted as somebody who has the ability to both pay and the inability to secure your network. And that can cost tens-of-thousands or millions of dollars, depending on the size of the company.

TCO: You said this doesn't really affect Macs yet. What is it that's inoculating Apple computers from this sort of ransom ware?

Jason: The Mac has always been more secure in general, simply because Unix was never really built for remote access like Windows was.

Anytime you want to do anything that modifies the system on a Mac, you have to put in an admin password. This makes it very hard to get a virus or malware on a Mac without you *allowing* it onto your machine. And that's where social engineering schemes like phishing come into play.

The only way malware succeeds is if you're tricked into putting in a password that allows it to run.

Apple also does a fairly good job of maintaining its XProtect database which it pushes out to end users on a regular basis, runs in the background, and keeps track of malicious information, and blocks those kinds of things from happening.

But it's not perfect, and that's why products like third-party antimalware, security, and antivirus programs exist, and why the companies that make them still service Mac clients.

But for the most part the reason is that it's a lot easier to leverage security holes on the PC than it is on a Mac, and since the install base is still so much higher, it's a more attractive platform to attack.

TCO: What do you think of folks who boast about being able to hack Macs in half a minute?

Jason: I'd say they probably have to be sitting in front of it. Doing a remote attack on a Mac is very very difficult. And in a real world scenario, given a choice between hacking one difficult Mac or ten easy PCs, hackers tend to favor the easy road.

TCO: So between XProtect, the obscurity of the platform, and various tools, it all boils down to users. They're the weakest link.

> "[Maybe] nothing happens for years, but they're maintaining the access and somebody's watching.
>
> And then all of a sudden there's an opportunity and they're going to jump on it."

Jason: Yep. It's about making sure that users just follow some basic best practices.

Have good strong passwords that are hard to hack.

Rotate those passwords on a regular basis.
Use a password management system so that people don't have just one password (nobody can possibly remember dozens or hundreds of complicated passwords). We need tools to help, and they're not expensive. So the third best practice is to use a password manager.

And just in case malware is inadvertently downloaded and installed, it's important to have good antivirus and antimalware software to catch it quickly and remove it.

It's not enough to just be skeptical, but you have to *run* tools on your system. And that includes backing up. Everybody should back up regularly and test the backups to be sure they're valid. It's the cheapest insurance anybody can get.

But Mac users, more than most, have a terrible habit of forgetting all that and just think, "Well I got a Mac, so I don't get viruses."

TCO: Those days are done.

Jason: Yeah, it's generally still an accepted fact, but even if Macs really were invulnerable, they could still be sleepers.

If there's a Mac on a PC network, that Mac can be an injection agent, a vector to get viruses onto the PCs even though the Mac itself is not affected.

TCO: Okay. To sum up, basically, the gist of our conversation, users should be skeptical and attentive, know what they're clicking on and read what the screen's trying to tell them. They shouldn't click links in emails, and instead manually type website addresses when there's a notification. Software should be kept up to date, security tools should be installed and kept running, and users should employ strong passwords.

Jason: That sounds about right.

TCO: Do you have any other thoughts you'd like to share in closing?

Jason: Users really need to consider everything outside of their computer as a hostile environment.

They need to dress accordingly. It's winter out there, and if you go out without a coat on, you're going to get frostbite. It's not the happy little internet that we all grew up with.

There's sharks in the water now, and you've really got to watch out for yourself. Be an informed consumer. Be cautious and be aware.

What is it in Latin, buyer beware?

TCO: Caveat emptor.

Jason: Caveat emptor.

TCO: All right, well thank you very much. I appreciated the conversation and the insights.

About Technology Revealed

Technology Revealed is the leading provider of Apple IT, Mac and PC support, and consulting services in Connecticut. Technology Revealed is a highly respected member of the Apple Consultants Network, employs a team of fully qualified Apple Certified engineers, and consistently earns rave reviews from its corporate and consumer clients. The company is headquartered in Milford, Connecticut with satellite offices in Hartford, Norwalk, Shelton, and Stamford.

Website: www.technologyrevealed.com
Email: service@trmacs.com
Phone: (203) 874-1468

Copyright © 2019. ALL RIGHTS RESERVED.

TECHNOLOGY REVEALED LLC