two river™
TECHNOLOGY TIMES

What's New

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords. Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is

an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access

with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better.

Digital Trends, May 7, 2020

November 2020

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

4 Questions Your IT Services Company Should Be Able To Say "Yes" To

Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT services partner – if you have a

Continued on pg.2

Continued from pg.1

partner – and tell them you need help. They might be able to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position.

And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to.

1. **Can you monitor our network and devices for threats 24/7?**
2. **Can you access my network remotely to provide on-the-spot IT support to my team?**
3. **Can you make sure all our data is backed up AND secure?**
4. **Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?**

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this

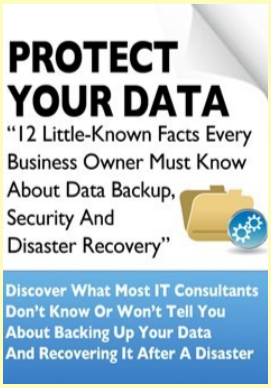
company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!"

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

FREE Report: 12 Little-Known Facts Every Business Owner Must Know About Data Backup And Disaster Recovery

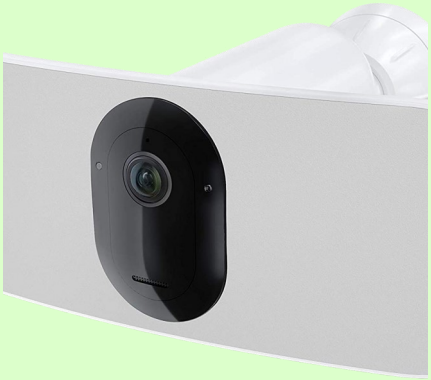


You will learn:

- The only way to know for SURE your data can be recovered if lost, corrupted, or deleted -– yet fewer than 10% of businesses have this in place
- Seven things you should absolutely demand from any off-site backup service
- Where many backups fail and give you a false sense of security
- The #1 cause of data loss that businesses don't even think about until their data is erased

Get Your FREE Copy Today by emailing your request to kmarquez@tworivertech.com

Shiny New Gadget Of The Month:



Arlo Pro 3 Floodlight Camera

In the era of porch pirates, more people are investing in outdoor security cameras. The Arlo Pro 3 Floodlight Camera delivers security and practicality. It features an ultrahigh-definition camera delivering 2K HDR video and color night vision combined with a 2000 lumens light. Nothing goes undetected!

Plus, the Arlo Pro 3 is wireless. It connects to WiFi and doesn't need a power cord (it just needs to be plugged in for charging periodically). Because it's on WiFi, you can check the feed anytime from your smartphone. You can even customize notifications so you're alerted when it detects a car or person. And it has a speaker and microphone so you can hear and talk to anyone near the camera. Learn more at: **Arlo.com/en-us/products/arlo-pro-3-floodlight.aspx**

4 Steps To Move Your Business From Defense To Offense During Times Of Disruption

"Everyone has a plan until they get punched in the mouth." –Mike Tyson

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant.

You have two options:

1. Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let's face it, that's not happening).
2. Create and act upon a new game plan. One that's built to overcome disruption and transform your business into something better and stronger.

Option Two is the correct answer! AND, we at Petra Coach can help.

At Petra Coach, we help companies across the globe create and execute plans to propel their teams and businesses forward. When disruption hit, we created a new system of planning that focuses on identifying your business's short-term strengths, weaknesses, opportunities and threats and then creates an actionable 30-, 60- and 90-day plan around those findings.

It's our DSRO pivot planning process. DSRO stands for Defense, Stabilize, Reset and Offense. It's a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn — better and stronger than before.

Here's a shallow dive into what it looks like.
Defense: A powerful offensive strategy that hinges on a strong defense. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

Stabilize: The secret to stabilization is relentless communication with everyone. That includes internally with your teams AND externally with your customers. Streamline communication and eliminate bottlenecks through a visual dashboard.

Reset: By completing the first two steps, you'll gain the freedom to re-prioritize and focus your efforts on the most viable opportunities for growth.

Offense: Don't leave your cards in the hands of fate. Shifting to offense mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

Interested in a deep dive where a certified business coach will take you (and up to three members from your team) through this process? Attend Petra's DSRO pivot planning half-day virtual group workshop. (We've never offered this format to non-members. During this disruptive time, we've opened up our coaching sessions to the public. Don't miss out!)

When you call a time-out and take in this session, you'll leave with:

- An actionable game plan for the next 30, 60 and 90 days with associated and assigned KPIs
- Effective meeting rhythms that will ensure alignment and accountability
- Essential and tested communication protocols to ensure your plan is acted upon

I'll leave you with this statement from top leadership thinker John C. Maxwell. It's a quote that always rings true but is crystal clear in today's landscape: "Change is inevitable. Growth is optional."

Let that sink in.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

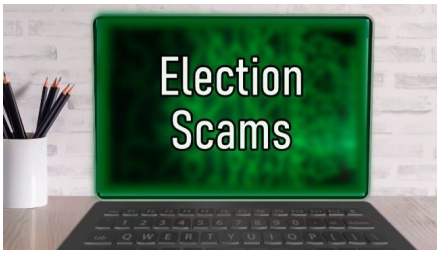
TRTG Happenings

2020 Leading Lights Gala

Two River Technology Group was happy to support our clients at Family and Children Services on an event they do annually to honor their heroes within. Normally, this event takes place at the Navesink Country Club where all the guests have dinner, dance and partake in an auction to benefit the FCS mission. However, due to COVID-19 and their concern of the safety of their staff and guests, FCS decided to make this a virtual event! On October 13th at 7:30 pm all guests who attended were able to participate in an online auction, raffle, and watch a video presentation! All guests had the option to pick up their dinners curbside at the Navesink Country Club and enjoy their meals from home.

Since 1909, Family & Children's Service, Monmouth county's oldest nonprofit social service agency, has been assisting people at vulnerable times in their lives through education, intervention, care and counseling. Events like this are very important as they continue to help support their mission and we were proud to be a part of it!

2020 Election Scams



The 2020 election is less than a month away. With millions of people voting, it's a perfect opportunity for thieves to trick people and take their money.

How are crooks targeting victims? Phone and email scams are the most common tactics. But this year, they're also leveraging social media to spread disinformation.

With so many election scams making the rounds, it's important to know red flags to look for. If you know how to spot them, you can protect yourself and avoid getting tricked. Here are 10 of the most common election scams you'll see in the next few weeks, along with how you can catch these scammers in the act.

1. Don't fall for fake campaign emails

Scammers are impersonating political campaigns by email and asking unsuspecting victims to donate money. If you make the mistake of opening one of these emails, you could end up on a phishing site that steals your data and credit card.

Even worse, you could end up downloading malware. Many of these scam emails instruct users to download what is really a malicious attachment that can infect their computer.

The messages sometimes contain professional graphic design and official campaign photos to look more legitimate. Some even spoof official email addresses owned by campaign staffers. They may also include urgent-sounding language meant to pressure you into sending money and data.

How to spot the scam:

- Avoid opening emails from senders you don't know or recognize. Even if an email looks like it's coming from a campaign, you're better off donating by visiting an official campaign website.
- Never download email attachments from senders you don't know.
- Check political emails carefully for spelling and grammar errors. These can be big red flags that the sender isn't actually working with a campaign (or American, for that matter).
- Always check the sender field. If the sender uses a random email address with a jumble of letters and numbers, ignore it. Legitimate political campaign workers will have email addresses ending in .com or .gov.

2. Watch for fake political websites

Fake political websites are growing in number as the election approaches. These websites are designed to look authentic, while stealing your personal and financial data. Some of them ask for campaign donations, while others ask you to sign up with your email address, phone number and credit card.

Spotting these fake websites can be tricky. Many of them use spoofed domains or slightly alter the spelling of real ones. For example, scammers may misspell election as "election" — or use .com instead of .gov. If you're not careful, these minor tweaks are easy to miss.

If you do fall for the trap, be prepared for the data you to end up on the Dark Web.

How to spot the scam:

- Never click on links you receive in unsolicited emails. Even if the link text looks normal, it's easy to disguise the real destination.
- Check the spelling of any URL you visit very carefully.
- If a political website asks for payment or personal information, don't share it — especially if you clicked from an ad or a link.
- If you want to donate to a campaign, visit the official website on your own through your browser. Don't click through social media, email or other sites to get to it.

TRTG Happenings

3. Always be skeptical about what you see on social media

Social media makes it easy for misinformation to spread — and it's only gotten worse during election season. The FBI has already detected a massive misinformation campaign underway right now designed to weaken trust in the election process.

The FBI says foreign and criminal actors are behind the campaign, and they're making claims that voter registration lists are being purged or hacked. Some are even saying altered or stolen voter registrations will prevent you from voting.

How to spot the scam:

- Social media scams are designed to provoke an emotional reaction. If you read something that makes you angry, anxious or fearful, ask yourself if that might be intentional.
- Claims about voter registration lists can be written off as fake. This information is easily obtainable, and campaigns get access to it all the time. Any claims that voter rolls are being purged or hacked are designed to make you distrust the process.

4. Beware of election ransomware

Fake campaign emails aren't just used for phishing. Some contain dangerous ransomware that can lock up your computer.

Scammers will send an email that looks like it originates from a campaign or PAC. If you click a link or download an attached file, ransomware goes to work scanning your computer and stealing your data. Then, it encrypts your entire hard drive with a password. To get everything back, you have to pay a ransom by Bitcoin — sometimes thousands of dollars worth.

How to spot the scam:

- Ransomware is generally spread through malicious email attachments. If you avoid downloading attachments, you're one step ahead.
- Scammers can sometimes use hijacked email addresses to share malware. If an email with an attachment comes from someone you trust, contact them first and confirm that they sent it to you before opening.
- Back up everything, often. Your best protection against ransomware is keeping your files updated. Even if they get access to your data, you can tell them to buzz off since you have copies of everything.

5. Don't give any money to these phone impersonators

Phone scams are all about impersonation. When scammers call, they'll usually claim to be working for campaigns, fundraisers or PACs. Some even pretend to be local officials or government agencies like the IRS or FBI.

The most advanced scammers rely on digital technology to make realistic-sounding recordings that mimic the voice of candidates. These spoofs can be hard to spot since they sound so close to actual recordings used by politicians. Regardless of who these callers claim to be, nearly all of these phone scams have one thing in common: bait and switch tactics.

If you speak with the caller, you may be asked to make a donation over the phone. Other callers promise a reward for answering questions in the form of a gift card. Once they're finished, they'll ask you to pay for shipping. If you give up this info, they take your credit card number and run.

How to spot the scam:

- Pollsters and campaigns rarely offer prizes. At this point, consider any political caller that offers you a reward a scammer.
- If a caller asks for any kind of payment information, hang up. Legitimate callers will not ask for this info.
- Ignore urgent or threatening calls. Scammers pretending to be the FBI or IRS may threaten to arrest you, but they cannot do this over the phone. If you hear this kind of language at all, hang up.
- Political callers will never ask for your Social Security number. Hang up the moment anyone asks for this.

6. Voting is free — don't let anyone tell you otherwise

Your phone rings and the person on the other end tells you that if you're not registered to vote, they can help you — for a price. If you work with the scammer, you're not just giving up your payment card info. You're also sharing your private voter info.

If you haven't registered yet, you can right now right from your desk or couch using these sites:

- USA.gov— Register to vote, find registration deadlines and read a guide for new voters
- Rock the Vote— A nonpartisan nonprofit that helps people register to vote and get involved

How to spot the scam:

- There is no cost to register to vote. It's free, and anyone charging to do it on your behalf for a fee is lying to you.
- Real get-out-the-vote campaigns want *you* to register personally. Don't trust anyone offering to do it for you.

7. No, you can't vote on social media

Just like the voter registration tactic, this social media scam uses confusion to trick people. Scammers post ads or share viral memes inviting victims to vote online instead of in person. This can be

TRTG Happenings

tempting since voting from home is more convenient. The pandemic makes this scam even easier to pull off.

To make matters worse, the links scammers share for online voting sites might take you to phishing websites instead.

How to spot the scam:

- Keep an eye out for spelling and grammar errors in social media posts. In 2016, some foreign-made election memes contained false information about voting by text — easily spotted thanks to common spelling errors.
- You can't vote online or by social media. Voting can only be done by official mail-in ballots or in-person polling.

8. Don't fall for fake voting tips

The COVID-19 pandemic has more Americans than ever interested in voting by mail. Unfortunately, scammers and election-meddlers are aware of this, too. That's why they're making an effort to share fake info about how the process works.

Some fake information may come to you by email or text message. Other scammers share it on social media to get the biggest audience as possible. Claims vary widely — from claims mail-in voting doesn't work to improper steps on how to do it.

How to spot the scam:

- Remember that voting by mail is safe and reliable. Millions of Americans, including many military families, rely on it every year.
- Refer to the U.S. government's official website for accurate information on how to vote.
- Confirm your voter registration through your local Board of Elections site.

9. These pollsters are not who they claim to be

Polls are a useful tool for gauging an election — but in the wrong hands, they can be used to sway public opinion. Some scammers are sharing fake polls while pretending to be campaign officials or third-party pollsters. These polls may include wildly inaccurate results that include one candidate losing by large margins against the other. The intent, of course, is to discourage you from voting.

Other pollster scams are less about the election and more about making money. These criminals will ask you to participate in a poll with promises of a reward. At the end of the survey, they'll ask you for payment information to ship you a gift card or other prizes. Sharing this info could lead to your bank account getting drained.

How to spot the scam:

- Be skeptical of any polls that lean too far one way or another.
- If a pollster offers you a reward for participating, hang up. It's probably a scam.
- Political pollsters should only ask for your party affiliation, voting preferences and some light demographic information. If a caller asks for your phone number, email address or physical address, it's a scam.

10. Snail mail scams can still happen

Don't count out snail mail just yet — because scammers are using it, too. Some are sending fake voter information with incorrect dates and instructions, while others are sending threatening letters demanding you pay to complete your registration. Regardless of what kind of letter you get, all of them have the same goal in mind: To trick you and steal your money.

How to spot the scam:

- Always check who sent the letter. If it's from a government agency, it will include an official seal and letterhead.
- If a letter claiming to come from a campaign asks for donations, don't follow the instructions in the letter. Instead, visit the official campaign website and follow the instructions online. If the letter is real, it all goes to the same place.
- What should I do if I fall for any of these scams?
- If you think you've fallen for a scam, don't panic. You have several options to protect your computer, yourself and others from harm:
- Install antivirus software to scan your computer for malware or ransomware. This can save your data and protect your information. Remember to scan regularly going forward.
- Disable or uninstall software you aren't using.
- Never enable macros on documents downloaded from an email unless absolutely necessary. If you have to, scan the file first to make sure it isn't malicious.
- Use strong two-factor authentication to protect your online accounts.
- Report any scams or criminal activity you encounter to your local FBI field office.
- Scams, by definition, are meant to deceive you. If you don't fall for them, you'll be safe. Make sure to share this with friends and family so they'll know what to watch out for in the lead-up to the 2020 election.