Issue 2 | Volume 7 | June 2021

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note

In recent times the human race has faced an unprecedented number of computer-generated offences, some of which have come about as a result of the effects of the Corona Virus. Due to new vaccination and the general state of the world because of the Global Pandemic persons have been bombarded with different conspiracy theories due to fear. Also, social distancing caused many to opt into online methods of ecommerce, meetings and general social interaction to combat isolation. Moreover, while working and studying at home persons have to be mindful of their surroundings. This quarter, our newsletter will look into various methods of securing one's self whether on/offline.

What is fake and what is real news, this question gets more and more difficult because almost 9 out of every 10 Americans admit to falling for a fake news story -- despite repeating warnings. But the real concern is how easily people are willing to pass this information to others, to the point where some of them are being described as "super spreaders." Article one discussed how not to fall for this. Most of the fake news in 2020 originated on the internet. What if your browser is misbehaving, showing unexpected ads and turning up weird results when you do a search? If so, you could be a victim of a browser modifier or hijacker. Read the second Article and you will be surprised.

In keeping in the theme of hacks Article three questions should you click that "unsubscribe" button at the bottom of those pesky spam emails that drop into your inbox by the score every day? Probably not, say email security experts -- because you could be lining yourself up for a scam or unleashing another torrent of even more annoying messages. And while many of us are working from home due to the current pandemic, criminals and scammers are also hard at work from home and have been increasingly more brazen since the stay-at-home orders have been put into effect. Articles four discusses how businesses can fight back against online scammers.

The final two articles explore your physical safety, the first one is about your vehicle and often times they are stolen and prospective buyers of smart devices ask whether GPS car trackers work. There are several GPS trackers on the market and the extent of their effectiveness depend on the individual features of the device. Finally we see that while everyone loves the ambience that decorative outdoor lighting provides, and the enhanced safety of illumination, many people simply do not make the right choices. As a result, the home and lighting system are off-balanced, which distracts from the beauty of the property. A well-lit home prevents home breakings but at the same time harsh lighting is a distraction, learn how to balance the two in Article six.

We do hope you find these articles and the safety methods helpful in some manner and we at **Amalgamated Security Services Limited** will continue to fulfil our commitment to provide quality service for all customers.

Regards
Carril Reyes-Telesford
Senior Marketing Officer

Almost 9 out of every 10 Americans admit to falling for a fake news story -- despite repeating warnings.

But the real concern is how easily people are willing to pass this information to others, to the point where some of them are being described as "superspreaders."

Whether or not you're a believer or spreader, you have an important role to play in guiding others away from the fake news trap, as we explain in this week's issue.

Let's get started...

Help Stop Fake News Superspreaders

It sounds like a contradiction but it's true: Fake news has become a fact... of life. And, despite all the warnings and counterattacks, it's getting worse. People, either thoughtlessly or maliciously, are passing on bogus news and doctored photos at a record rate.

Technical experts are trying to create artificial intelligence (AI) formulas to detect and remove it. Meanwhile, organizations from political groups to academics are getting seriously worried.

Psychologists want to understand why we do fall for fake news and pass it to others. As with contagious diseases, security experts are starting to talk about misinformation "superspreaders" -- people who unhesitatingly post and forward messages to hundreds of other friends and online followers.

A massive 86 percent of us admit to falling for fake news at one time or another. And research shows that in any single year, around half of us believe in one or more conspiracy theories.

Yet, the vast majority of us -- 83 percent -- say they're worried about myths, misinformation, and fake news. We know from hard experience -- such as people swallowing unsafe "curatives" -- that it can be downright dangerous.

We also know that if a report or post aligns with our own opinions, we're more likely both to believe it (a tendency called "confirmation bias") and then to pass it on without question.

Social media sites take the crown for being the riskiest sources for the circulation of fake news and conspiracy theories because of the sheer number of people who use them. That's where the superspreaders lurk.

Even if you're not a fake news spreader yourself, you can play an important role in helping to stem the tide of misinformation. You'll almost certainly know of others who do forward fake reports and claims, maybe among family or friends.

Here are 5 tips for helping others who fall into the fake news trap from the freedom-of-expression organization PEN America:

1. Try to check and verify something you suspect is fake news before engaging with people you know who are passing it around.
2. Think carefully before commenting publicly on a fake item. It may help others, but it could also misfire by raising the visibility of the fake news or opening a damaging debate.
3. Be sensitive to how spreaders might react. It can be embarrassing to be "caught out" passing. Try to imagine their

perspective. Be positive and supportive when you open a discussion. Don't ridicule them.

4. If they react badly or defensively, don't pursue or escalate the discussion. Explain how they can fact-check. And get in the habit of providing sources when you pass information to them.
5. Try to help educate them. Pass on information and tips on spotting and avoiding fake news and let them know you're a resource -- available to help if they're uncertain whether something is true or not.

Improve Your Own Behavior

And here are a few more things you can do to improve your own understanding and behavior when dealing with potential fake news:

- Be honest. When you present or report on a topic, stick to known and checkable facts and, if you can, give the source. If you believe something to be true but can't verify it, make that clear when you relate it to someone else. Research also shows that by presenting the true facts first, people are less likely to believe subsequent reports that say otherwise. This is known as "prebunking."
- Read the experts. Dozens of academic experts in the field have also produced a "Debunking Handbook" to help people avoid spreading misinformation. It's a bit scholarly, approaching the subject from a scientific and research perspective. But there are some useful tips -- and it's free! Download a pdf version here: https://tinyurl.com/scambusters-210523-1
- Also check our previous Scambusters' reports on how to identify and avoid fake news and other related scams. Start here: https://scambusters.org/?s=fake+news

How to Beat Browser Modifier Scams

How's your browser? Is it misbehaving, showing unexpected ads? Turning up weird results when you do a search? If so, you could be a victim of a browser modifier or hijacker. These are pieces of malware that change the way your browser looks, inject ads onto some pages and into search engines, slow down your computer, and generally make web surfing a frustrating experience. They're downloaded onto PCs via email attachments, Internet links, and even by what are known as "drive-by downloads" -- where malicious code is hidden on a web page and sneaks onto your PC when you visit.

The latest and most widespread of these is a group of browser modifiers called Adrozek. It was identified last year and hit a peak in December and this past January. And even though most Internet security software now detects it, users who don't use or haven't updated this software, or who were infected some time ago, could still be

suffering.

Adrozek installs extensions -- mini programs designed to improve the operation of browsers like Edge, Chrome, and Firefox. It also modifies some of a browser's computer code, including security preferences, turns off browser updates, and then changes settings to show advertisements. Sometimes, the ads overlay genuine ones.

With some browsers, the malware is even capable of stealing user information and sending it back to the scammer.

In a recent warning, tech giant Microsoft said users, while searching for certain keywords, may click on them. In most cases, the links lead to affiliate pages that pay the scammers for each click, but they could also be used to install further malware onto a PC.

"Cybercriminals abusing affiliate programs is not new -- browser modifiers are some of the oldest types of threats," says Microsoft. "However, the fact that this campaign utilizes a piece of malware that affects multiple browsers is an indication of how this threat type continues to be increasingly sophisticated. In addition, the malware maintains persistence and exfiltrates website credentials, exposing affected devices to additional risks."

Hundreds of thousands of machines are said to have been infected globally and security experts fear the malware will spread because of the complex infrastructure developed by the scammers, which involves millions of unique Internet addresses (URLs) from which Adrozek is launched.

As Microsoft suggests, browser modifiers have stood the test of time -- which means that they must be effective. Some, like Adrozek, use a tactic known as polymorphism to change their structure after installation to avoid detection.

There are numerous varieties. And scammers use sneaky tricks to get you to install them. For example, they may use a pop-up with a "cancel" button. Clicking it downloads the malware.

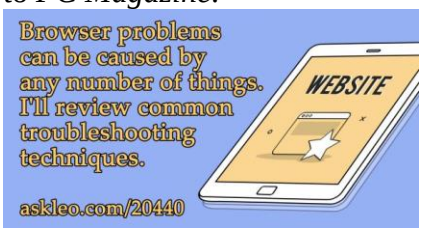
Has My Browser Been Modified?

How can you tell if you have a browser modifier?

Well, the first sign is that unusual behavior we talked about earlier. The most obvious sign is that your home page -- the one that appears when you open the browser -- is different from the one you set up. Some modifiers also change fonts and other elements of the browser's appearance. And, of course, if you install or update good security software, it should also be able to detect most modifiers.

Generally, any unexplained, erratic or slow behavior by your browser could indicate the presence of one. You can also check your browser's automatic update setting to see if it has been switched off.

More experienced users can look in their "Programs Files" folder for names they don't recognize. In the case of Adrozek, these include audiolava.exe, quickaudio.exe, and converter.exe, according to *PC Magazine*.



In addition, you can check your browser's "extensions" page to see if there's an add-on listed that doesn't appear in your toolbar.

Defend Yourself Against Browser Hijackers

So, what can you do? Here are five important actions.

1. First, avoid installation in the first place by using and updating your Internet security suite and ensuring it checks sites and files in real time. Run scans regularly.

2. Second, don't click on pop-ups. With some browsers, they can be disabled totally. But when one appears, simply close the tab or even the entire browser.
3. Remove/delete/uninstall any browser extensions you don't recognize. This is a good practice for security in general.
4. If you are downloading software, only use reputable sites. Some browser modifiers are hidden inside software bundles, especially those offering free downloads.
5. It may be possible to uninstall a modifier, but it's usually best to remove and reinstall the entire browser. It's a good idea to regularly back up your browser's settings (but not if it's infected!) so you can reinstate them after a reinstall.

You'll find lots more information on individual browser modifiers and uninstallation here: https://tinyurl.com/Scambusters-210507-1

What's especially worrying about Adrozek, say the experts, is the level of sophistication, including distribution and polymorphism. Microsoft says this means it will grow further in the coming months.
Reprinted from Scambusters.org

Don't Click that Spam Unsubscribe Button!

Should you click that "unsubscribe" button at the bottom of those pesky spam emails that drop into your inbox by the score every day? Probably not, say email security experts -- because you could be lining yourself up for a scam or unleashing another torrent of even more annoying messages.

An estimated 54 billion -- that's 54 thousand million -- spam mails are sent out worldwide every day. It's a numbers game. Spammers know that a tiny, tiny fraction of that number will hit home and hook their victims. But they're greedy. So many of those messages end up at unused addresses. Or they get weeded out by spam detectors in your Internet security app. If only they knew which mails were getting through and being read by users.

Why not put a button inside the message and lure recipients into clicking. Let's call it "unsubscribe," they cunningly think. The frustrated user clicks the button or a highlighted "unsubscribe" link at the bottom of the text. Hey presto! They just told the spammer: "I'm here and ready for more."

This isn't valuable just to the spammer either. The user's address goes onto a list that can be sold to other spammers. So, instead of getting rid of the rubbish, you just invited more of it to pour into your inbox.

More worrying is that some "unsubscribe" links are actually triggers for downloading malware onto your computer.

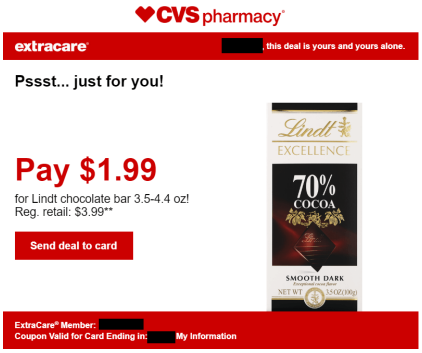
For example, recently, spammers have been sending out messages seemingly linked to adult and dating websites -- with a prominent "unsubscribe" button linked to malware. They know recipients are highly likely to hit it because it'd probably be embarrassing if anyone else saw it.

In other, similar cases, users who click these links are presented with a form to fill in, which is really just a thinly-disguised attempt to steal information. Initial emails may even be spoofs, appearing to come from a reputable organization, and tricking unsubscribers into giving away confidential information such as passwords.

Spot the Differences

There are also many legitimate news and marketing emails that offer a genuine opportunity to unsubscribe. But how can you

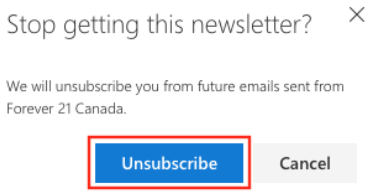
tell the difference between those and the baddies?



Of course, you want to limit the flow of messages into your inbox. In a perfect world, you'd only get the stuff you want. To get nearer to that goal, here are some of the actions you can take.

- Check if an unwanted email comes from an address or organization you actually subscribed to. If so, you can probably safely select any unsubscribe option, but it's important to check the sender's address to be sure it's not a spoof as outlined above.
- Watch out for misleading statements at the bottom of a message saying that you previously subscribed to the sender or an associated business. This can mean your address has actually been passed around between different organizations. If you don't remember signing up, it's better not to click the unsubscribe link.
- Use an email service provider that filters out spam at the source. Gmail is a good example of that. The service removes suspected spam before it even gets into your inbox. You can check the online Junk Mail folder now and then to make sure a genuine message didn't end up there.
- Use your email client's (program's) built-in junk filter. Again, many online and desktop email apps have slide-type settings that enable you to select how strictly you want them to automatically remove suspected spam.
- Manually trash any spam emails that you spot and let your app know that it's junk by clicking on the appropriate button.
- Set up spam selecting rules. Again, you can do this with many email apps such as the desktop version of Outlook. For example, if you keep getting rubbish from a known spammer, instruct the app to always move items from their particular address to your junk folder.
- Be cautious about who you provide your email address to. For instance, you can use an instant, temporary email address for any new service you subscribe to and only change it to your real address once you're happy with their messaging. Do a browser search on the words "temporary email address" or use similar terms such as "one time" or "instant," to find one of these services.

Always confine your main email address to friends and others you trust and have separate ones for activities like shopping.

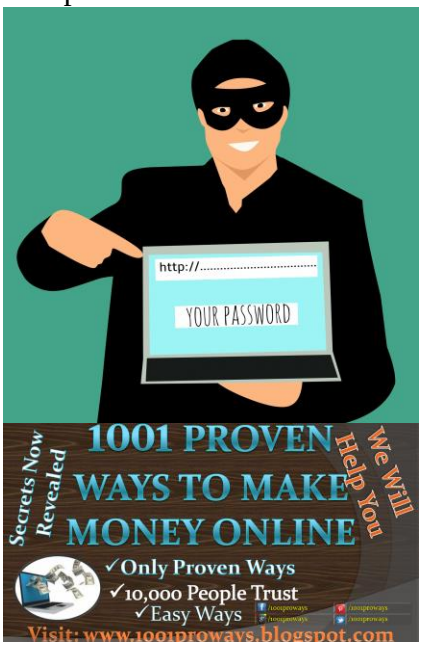


For more information on unsubscribe scams and spams, check out this useful article from the non-profit Identity Theft Resource Center (ITRC): https://tinyurl.com/Scambusters-210114-1
Reprinted from Scambusters.org

How businesses can fight back against online scammers

Despite the pervasiveness of phishing and catfishing schemes, organizations can use the UDRP process to regain the upper hand

Philip Nulud



While many of us are working from home due to the current pandemic, criminals and scammers are also hard at work from home and have been increasingly more brazen since the stay-at-home orders have been put into effect. In popular media, we see television shows such as "90 Day Fiancé," "Catfish: The TV Show," and others depicting people being scammed by unscrupulous individuals online who are pretending to be someone they are not. Those scams are often colloquially referred to as phishing or catfish scams. Not only do these scams affect and target individuals, but they also target businesses.

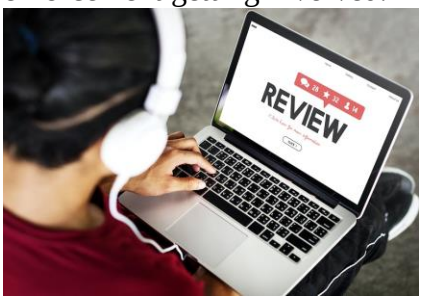
We have seen businesses, including law firms, be targeted with false emails from people purporting to be the CEO of the business asking someone to "do them a favor" and buy gift cards or wire money. However, while people are more keen on these scams, there are much more complex scams. For example, scammers have registered domain names that appear to be similar to a company's domain name. They will add an extra character to the company's domain name or trademark, or make an easily made mistake such as substitute "nn" in the domain name to an "m" or change a "t" to an "f" and therefore create a false, but official looking domain name or one that is easily mistaken with the official domain name. For example, I own the domain name nulud.com, but a scammer could create the domain name mulud.com or nu1ud.com and try to purport to be me. Creating such a domain name is not difficult, nor is it costly, which is why these scams are prevalent.

What I have personally seen as an attorney for some of these businesses that have been unfortunate targets of such online scams is that the scammer first creates a false domain name similar to the company's own official domain name or trademark. Then, they create an email address using that domain name that impersonates a company executive (since typically that information is public). Using that false email address they then ask an employee or employees of the company or clients of the company for some innocuous information such as a report of accounts receivable. Once they receive this report, they contact the people on the report that may have outstanding balances using the false email address (or they create an additional email address to appear like the person that they obtained the information from). They then ask that the person wire the payment to a bank account that the scammer controls. Thankfully, most people have been able to spot the scam and have averted disaster.

A similar type of scam involves the creation of a fake store that impersonates the business. They create a domain name using the business' trademark, often times adding a descriptive term such as "store" or "clothing" (or whatever the business sells). This creates a domain name that appears to be related to the business. The scammer then

creates a false website that is usually a virtual copy of the business' own official website. They then purport to sell the business' goods at a significantly discounted price to consumers. Typically, they do this to steal consumer's credit card information (this is referred to as phishing) or to sell poor quality knock-offs of the business' goods. Either way, not only does it hurt consumers, but it also hurts and disrupts the business and the goodwill they have established under their trademarks.

If one of the aforementioned scams occurs, there are various ways a business can take action. They can contact and work with law enforcement or they can ask their attorney to get involved. While local, state, and federal law enforcement has the most amount of discretion and can handle these types of cases, they oftentimes do not have the bandwidth to do so. What I have done as the attorney in this situation is to enforce the business' trademark rights and issue letters to the registrar the false domain name is registered under and/or file a Uniform Domain Name Dispute Resolution Policy (UDRP) complaint to take control over the false domain name. A UDRP is an out of court administrative proceeding that is decided by an arbitrator and enforced on the registrar (unless one side appeals). The UDRP can either remove the registration of the domain name from the current owner or it can transfer ownership of the domain name to the plaintiff. Oftentimes, this is faster or as fast as law enforcement getting involved.



With a UDRP, one has to prove that 1) they have trademark rights and that the registered domain name is identical or confusingly similar to the trademark which they have rights in; 2) that registrant of the domain name has no rights or legitimate interest with respect to the domain name; and 3) that the domain name was registered and being used in bad faith. The UDRP process is a usually a one shot, one complaint, affair in which we establish the trademark rights and aforementioned elements, give the other side a chance to respond, and then an arbitrator issues a ruling. Action can occur in as early as thirty days. The remedy is that the client obtains control over the false domain name, locking out the scammer and preventing them from scamming more customers related to the company.

There are many different nuances with regard to the UDRP process, the required elements, as well as trademark rights. We recommend that you speak with an experienced attorney to discuss your potential claims.

About the Author:

Philip Nulud is an experienced intellectual property attorney at Buchalter. He has successfully represented many businesses from fashion brands to well-known celebrities and musicians in recovering hundreds of false domain names as well as establishing and protecting their trademark rights worldwide.

Reprinted from SecurityInfowatch.com

How Does a GPS Car Tracker Work?

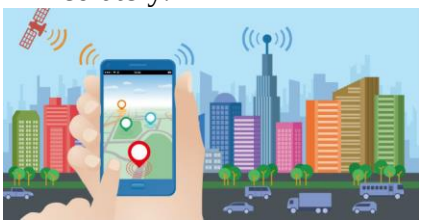
By Osric Griffiths

How Does the GPS Car Tracker Work?

Often times vehicles are stolen and prospective buyers of smart devices ask whether GPS car tracker works. There are several GPS trackers on the market and the extent of their effectiveness depend on the individual features of the device. Some will automatically shut down the vehicle after driving for a certain distance, while others automatically alert the police while its GPS capabilities allows the vehicle to be tracked. If one is operating on a budget, purchasing an intelligent car tracker might be the best decision to make as a motor vehicle owner. Here are few important features one should look for when deciding whether to purchase a GPS car tracker.

Alert System- Your system should be able to immediately alert you if your vehicle moves without your permission. Having the number for the nearest police station is always suggested or if you know a police officer, have his or her number on speed dial. Often times car thieves are caught in their tracks while in transit or when being pursued by police officers.

Tracking - The only way to retrieve a stolen vehicle is to know where it is located. The GPS car tracker should have the latest computer aided chip that is designed to connect with a GPS satellite to give the exact whereabouts and directions to the stolen motor vehicle. It is also suggested to have the device discreetly installed in a socket in the vehicle so that it cannot be easily detected and removed if the vehicle is stolen. As soon as the vehicle is picked up on the tracker, the police should be informed immediately.



Analytics- So the vehicle is identified and is tracked but what took place between the time it was taken and when it is retrieved by the police? There might be further clues as to the whereabouts of persons involved based on the stops made during theft. The intelligent sensors should be able to monitor and record abnormalities that happened to your vehicle's system. If there are missing parts, it should highlight the discrepancies.

Safety- Although identifying and nabbing car thieves sounds like a good thing, it could pose a threat to one's life. If there is an engine demobilizer attached to the GPS system, it is suggested to have a delay mechanism which allows the vehicle to drive for a period before it is disabled. In the event someone is carjacked, there should be some distance between the owner and the getaway driver. This short time will allow the owner to seek help or move away to a safer and more secure spot.

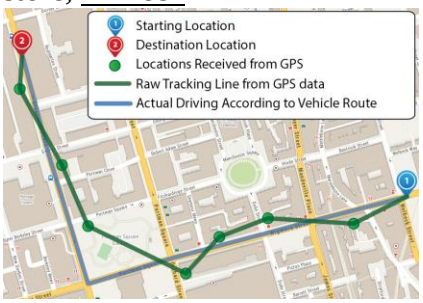
The Overall Purpose of a GPS Car Tracker

If one's vehicle is out of sight he or she will have peace of mind-knowing where it is and who took it. It also provides an alert system that notifies security personnel or the owner. Another purpose of the GPS car tracker is that thieves are normally discouraged when they believe there is a GPS car tracker installed in a vehicle. Once there is a GPS tracker, the chances of reclaiming the vehicle before it is dismantled are significantly increased.

Additionally, with a GPS system in your vehicle you can gather information about how designated drivers used the vehicle. If you have teenagers driving your vehicle one is able to monitor speed limits and

whereabouts of the car. It also helps in locating your vehicle if you have forgotten where you parked!

When considering an effective GPS car tracker, you may want to visit our online electronic store, Hi Tech



Offers. With iTrack GPS Car Tracker, vehicles are tracked in real time and have speed monitoring and route tracking capabilities. It also compatible with Android & iPhone devices. Click here for more details.

Article Source: https://EzineArticles.com/expert/Osric_Griffiths/1234879

If you are interested visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Tips for Choosing Decorative Outdoor Lighting

By Lydia Quinn

If you were to drive around any neighborhood while paying close attention to decorative lighting, you would begin to notice a pattern of gorgeous homes with lighting systems that are too small or cheap in appearance. On the other hand, you would begin to see smaller homes where homeowners had installed oversized lighting systems. In other words, while everyone loves the ambience that decorative outdoor lighting provides, and the enhanced safety of illumination, many people simply do not make the right choices. As a result, the home and lighting system are off-balanced, which distracts from the beauty of the property.

The goal when buying decorative outdoor lighting is to have a plan, which would include the size and style of home. From there, you would find it much easier to purchase a lighting system that would enhance and complement the home rather than create an awkward appearance. One of the next steps is to determine the appropriate size of outdoor lighting for your needs. Keep in mind that no hard rules exist as to size, walk outside, and standing at roadside look at the home. Try to focus on any architectural features that stand out such as a lamp post, statue, pillars, etc. Using good visual judgment, determine the size of decorative outdoor lighting that would create balance.

Another important aspect of choosing decorative outdoor lighting has to do with illumination. Typically, you want the exterior to be lit up for security reasons but you also want to avoid harsh glares. Therefore, we recommend you again look for decorative outdoor lighting that provides balance. After all, this type of lighting should be fully functional.

If you plan to place light fixtures along a driveway or upstairs leading to the front door, illumination should be bright enough to make walking safe while at the same time not so bright that illumination is actually distracting. If you need brightness, then it would be better to illuminate a broad area so the light is not so concentrated. Most decorative outdoor lighting systems come with a minimum of 100-watt capacity, whether as a single light or multiple lights. For creating light outside, this is plenty.

In addition to size and illumination, you want to consider the material of the decorative outdoor lighting fixture. Today, the five most popular choices include iron, brass, copper, cast aluminum, and composites. Although there are other options, these are used because they can withstand the elements and remain beautiful and functional. The hardest material to find is cast iron but something hand-forged would be gorgeous. Just be sure the metal parts of the system are zinc coated to eliminate rust from developing.

Brass is a popular choice simply because it has an elegant look. However, decorative options made from brass also ensures a long lasting system that can handle all types of environments. The only exception is that brass does not handle extreme heat but choosing fixtures that have powder coating would eliminate any concern. It would also be worth spending a little more for solid brass. No matter the choice, brass does go through a unique oxidation process whereby the surface color changes but for decorative outdoor lighting, it adds to the charm.

Even if you were on a tight budget but desperately want new outdoor lighting, remember that companies have sales all the time but you could also make your purchase directly from a manufacturer. In addition, we suggest you look at options for decorative outdoor lighting online. Because companies that sell only via the internet do not have the same high overhead as brick and mortar companies, it is possible for them to pass incredible savings on to the customer.

Visit BrandonSafetyLights for the best in traffic safety supplies: http://brandonsafetylights.com

Article Source: https://EzineArticles.com/expert/Lydia_Quinn/29438