COMPUTER NEWS from the

December 2013 Volume 1 NO. 12

As found on the web and other sources

IPads, iPhones, and WiFi hot spots everywhere

What is a person to do?

Avoid These Five WiFi Security Mistakes

FROM “askbobrankin,com”.

WiFi networking is convenient and liberating, and essential if you have a laptop or tablet. But if you aren’t careful, using wireless Internet can leave you open to hackers and unauthorized moochers of your Internet service. Here are five of the biggest mistakes that people make with WiFi, and how to avoid them. Read on!

Is Your WiFi Wide Open?

Several years ago, I got Verison's FIOS high-speed Internet service at my home. And then something curious happened. Cars were stopping in front my house, and staying for 10 or 20 minutes. There's no reason for anyone to stop there, so my spider sense began to tingle. After checking my wireless router, I found that Verizon had left it wide open. Without a wifi

password, anyone could connect! I locked down the router's wifi signal with a password, and the daily stream of cars stopped.

MISTAKE #1: Failing to put a password (also called an encryption key) on your WiFi lets anyone within range of your wireless router join your network. If file and printer sharing are also enabled, random passersby may be able to sift through files on every computer on your home or office network. Unencrypted WiFi also allows eavesdropping on your Internet traffic, even if the snoop is not connected to your network. Data passing between a computer and a wireless router is broadcast in all directions as far as several hundred feet.

Moochers on unsecured WiFi networks may slow the traffic of authorized users, or even download illegally while leaving the network's owner with the legal consequences. For these reasons, it's vital to set up your wireless network to use one of the encryption methods built into all wireless routers.

MISTAKE #2: While you're locking down your wifi signal, don't make the mistake of choosing WEP encryption, the oldest and weakest encryption method. It can be cracked in about two minutes using software easily found online. Unfortunately, WEP is often the first option on a router's list of available encryption methods, so don't be lazy and choose it for that reason. Use WPA2 encryption with the Personal (PSK) option, for the best protection.

(See my related article Is Your Wireless Router REALLY Secure? to learn how a couple in Minnesota almost got framed for harassment, trafficking in child porn, and threatening the Vice President -- all because they used WEP encryption on their wireless router.)

MISTAKE #3: Weak encryption keys (passwords) are a related mistake. Strong encryption is of no use if a hacker can obtain your password by brute force attempts or by guessing it. Some wireless routers come with a default (factory set) password like "admin" or "password". And

sometimes, internet service providers will set your wifi password to your home phone number. Passwords like these are trivial for even the most clueless hackers to guess. It's also common for the router's login credentials and/or wifi password to be listed on a sticker applied to your router.

Let me clear up a common point of confusion here. Your internet router has a username and password that you'll need if you want to login and change any settings. One of those settings is the wifi password. So there are TWO passwords being discussed here, and both are important. Your Internet Service Provider should have given you the router's username and password, if they supplied the router. Otherwise, look for it in the manual that came with your router.

Strong passwords should be at least 12 characters long and include a mixture of upper/lower case letters, digits, and special characters. For example, the password "M@ry Had a L1ttl3 L4mb" is a much better choice than "123456" or "qwerty". You needn't worry about entering this password over and over. Typically, you'll only need the wifi password when setting up a new device such as a laptop, tablet, smartphone, or wireless printer. (See Hey, Is This Your Password? to find out if your password is one of the 25 most common and easily guessed.)

MISTAKE #4: Disabling the firewall built into most modern routers in hope of getting faster Internet is a fourth mistake. Firewalls keep unauthorized outsiders from getting into your network. They do not appreciably slow your Internet connection. Do not disable your router's firewall. (See Do I Really Need a Firewall? to learn more about firewalls.)

MISTAKE #5: Relying on stealth alone to escape hackers' attention is a mistake that some people make. Some people think that they can get away without encryption or a password on their wifi, just by hiding their wifi router's SSID. Yes, most routers have a setting to disable the broadcasting of the router's SSID (name) so that other WiFi users within range won't "see" it on the list of available wireless connections.

Disabling the SSID isn't a bad idea. It will make your wifi signal invisible to most casual passers-by. But the SSID is included with many kinds of Internet traffic, so a hacker with free "sniffer" software can intercept and discover your router's SSID. Similarly, using MAC address filtering to allow only specific devices to connect to your network isn't a reliable method either. MAC addresses are easily spoofed and, like SSIDs, are embedded in Internet traffic that can be intercepted. MAC address filtering is a good supplementary security precaution, but do not rely on it alone.

BONUS: If you have a router that has the WPS (Wifi Protected Setup) feature, your router may be vulnerable to unauthorized users. See my related article WPS Security Flaw: Are You Vulnerable? to see if you are affected, and how to fix the problem if necessary.

If you want some additional tips on wireless security, or information about how to login to your router to change security settings, see my Wireless Network Security Checklist.

Read more:
http://askbobrankin.com/avoid_these_five_wifi_security_mistakes.html#ixzz2l3KZH7Ot

---

Phone Scam Resembles CryptoLocker Ransomware

By Brandon Dimmel on 20131125 in "infopackets.com".

The new 'CryptoLocker' Ransomware scam has been causing havoc online for the past few weeks. But you should also be aware of a similar scam being carried out over the phone instead of through emails.

Here's how the scam works: first, targets get an unexpected call from an unknown caller located within their area code.

If the call is answered, the caller tells the target that they're from a reputable tech firm, such as Microsoft or Dell or even a security company like McAfee or Sophos.

Usually the caller claims to be "working with" (rather than for) the named firm, often in the tech support department. (Source: sophos.com)

Scammers Use Minor Error Messages to Frighten Targets

Next, the caller informs the target that their computer has a virus of some kind and that this problem needs to be addressed as soon as possible. In some cases, the caller may place a great deal of pressure on the target in an effort to get them to behave.

Reports indicate that those people who put up a fuss -- say, by asking for more information -- usually hear a "click" as the call terminates.

But for those people who don't hang up, the caller will ask them to open the Windows Event Viewer. The caller will then try to help the target find any error message and then try to convince the target that this represents a serious security issue.

Scammers Demand $300 Fee For Fake Cleanup

The next step involves the caller convincing the target to give them remote access to the "infected" PC. The caller may then point to other minor error messages as a sign that the computer is laced with some kind of malware.

Finally, the caller will offer the target a system cleaning in exchange for a $300 fee.

Security firm Sophos says most of the scam calls have originated in India. Many of the companies behind the scams have reportedly ignored Do Not Call lists, meaning they continue to call a home even if they're dismissed. (Source: sophos.com)

The Federal Trade Commission (FTC) is investigating the problem, but in the meantime it's important everyone take a great deal of caution when receiving calls from a "computer expert". (Source: ftc.gov)

Can VoIP Service Replace Your Landline?

From “askbobrankin.com”.

A reader asks: 'I have a landline and a cell phone, so I'm thinking of dropping the landline phone in favor of VoIP phone service, to save some money. What is your opinion of VoIP, and what are the pros and cons of using it to replace a traditional landline?'

Is It Time to Drop Your Landline?

In tough economic times, folks are looking to cut expenses any way they can. Many are even eyeballing that telephone handset on the counter, wondering if they really need a traditional wired landline anymore. Quite a few have decided that they don't, opting to replace it with VoIP telephone service, which uses an Internet connection to make and receive phone calls. Is VoIP (Voice over IP) the right choice for you?

Let's start by de-geekifying the terminology. When you see “VoIP” or “Internet telephony” just replace it in your mind with “Internet Calling.” In a nutshell, here's how it works. VoIP connects your phone to the Internet via your high-speed internet connection (DSL, cable or fiber optic.) Instead of plugging into your local phone company's wall jack, you plug your phone line into a VoIP adapter. The adapter plugs into your computer or Internet modem/router and converts the signal from your phone into data that travels over the Internet.

The advantage of these VoIP services is that you can pay a lot less, and you don't have to change anything about the way you make and receive calls. You'll continue to use the same telephone handsets, and in most cases, you can even continue to use the same phone number.

The landline market in the U.S. has been shrinking steadily for about ten years. The number of homes with a landline only is now below 8%, and some phone companies are mulling whether it's time to stop offering landline service altogether. Two newer technologies are replacing landlines: cellular phones and VoIP .

By comparison, the residential VoIP market is young. Vonage, one of the oldest players, was founded in 2001. Vonage has about 2.5 million subscribers worldwide. Most analysts agree that residential VoIP started taking off in 2004, when cable companies such as Comcast and Time Warner began to offer bundled services including VoIP, TV, and Internet access. Over 90 percent of residential VoIP "lines" are provided by cable companies.

For those who already have high-speed internet (DSL, cable or fiber), dropping that expensive landline can be very tempting. The unpredictability of the monthly phone bill, along with all those mysterious taxes and fees, bring many consumers to a boiling point. Vonage offers unlimited local and long distance calling in the U.S., Canada and Puerto Rico for $24.99 per month. Comcast, Time Warner, Cox, and other service providers offer flat-rate VoIP calling at similar price points.

Other options such as Skype, Google Voice and Magic Jack offer VoIP phone service for less, and even for free in some cases. See my related articles Free Internet Phone Calls and Magic Jack Phone Service to learn more about these alternatives.

Switching to VoIP: Pro and Con

Cost alone does not dictate that everyone should ditch their landlines for VoIP. VoIP is more vulnerable to power outages than landline service is. The traditional telephone wires are powered separately from the general electrical grid. So when the lights go out, your landline will probably

still work. That's one good reason to keep a landline even after adding VoIP service. But the problem is also solved by having a mobile phone, at least until the battery runs out.

The 911 emergency service works very consistently with landlines, but can be problematic with VoIP. A landline terminates at a fixed location. When you call 911 from a landline, your location is automatically and surely transmitted to the emergency response center. But since they are not traditional phone services, VoIP providers do not have to provide emergency 911 calling. However, many of them will enroll you in what's known as Voluntary 911 Service. VoIP providers can use your billing address, or provide you with some other means of giving your physical address, which is used to associate your phone number with your physical location, in the emergency 911 database.

If you move, or you temporarily change the location of your VoIP phone, it's your responsibility to update the E911 address location information. And of course you won't have the ability to make 911 calls in the event of an Internet connection failure, or if you lose electrical power at your location. You should always have an alternative means of accessing 911 or similar emergency services, such as a landline telephone, mobile phone or a neighbor. Some people just don't want that kind of uncertainty when their lives may be on the line, so that's a consideration when deciding whether or not to go with a VoIP-only phone solution for your home.

A good inexpensive compromise might be VoIP service backed up by a prepaid or pay-as-you-go cell phone.

Read more:
http://askbobrankin.com/can_voip_service_replace_your_landline.html#ixzz2kjB1X5qx

---

The AskBobRankin Geekly Updates

Whip out your camera, it's time for a selfie! The folks at Oxford Dictionary have chosen "selfie" (a self-photograph, typically taken with a smartphone, and uploaded to social media) as their 2013 Word of the Year, but bitcoin, twerk, fatberg, schmeat, frankenburger, and sharknado all got honorable mentions.

"Who's watching the watchers?" Samsung Internet-enabled “smart” TVs have a security hole that would enable remote viewers to watch you in your living room. It’s just one of many examples of “smart” appliances that have absolutely no security features built into them.

Quote of the month:

Just because you do not take an interest in politics doesn't mean politics won't take an interest in you!
-- Pericles (430 B.C.)