UltimateITGuys.com

2017 Housing Authority Technology Guide

We are The Technology Service Provider for Housing Authorities!

Let Us Start Helping You!

UltimateITGuys.com

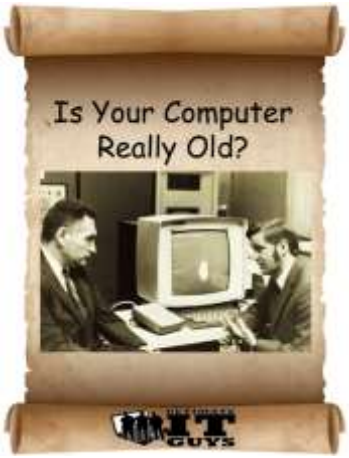
2017 Housing Authority Technology Guide

1. What to look for in a new computer
2. Being Safe Online - Don't be a victim (Avoid scams, malware & phishing)
3. Standard Best Practices for setting up your computers
4. What is the Cloud and is it safe?
5. How to keep your computers working
6. Identity Theft—Protecting you, your employees & your resident's information
7. So You Want a website
8. You've Been Hacked!
9. Free Email Could Cost You Everything
10. How to go mobile, without losing your mind

Ultimate IT Guys, The Cure For Computer Stress!

UltimateITGuys.com

What To Look For In A New Computer



Here are a few quick things to help you purchase your next computer.

Typically, you should replace your computers every 3-5 years. While It is possible to get longer use, at the rate that technology changes today, you will suffer from lost productivity and added expenses to maintain them after that point.

A computer is a tool that you use every day in your business, so treat your computer purchase as an investment in your business. Get the right tool for the job and you will be much more satisfied than if you just run down to Walmart and get the cheapest thing you can find.

BASICS

Brand

It is best to stick with name brand computers. In today's world that is **Dell, HP or Lenovo**. There are many other companies that make computers, but for a business class PC stick with these three companies and you will have better maintainability, compatibility, supportability and lower costs over the life of the computer.

Processor

Now that you know what brand you need, it is time to focus on the specifications of the computer. The best processor series right now is the Intel "I" series processors. These will be designated at i3, i5 or i7. **For most business applications, we recommend the i5 processor**. It is the best combination of power, performance and cost.

Memory & Hard Drive

Computer memory and hard drives are similar to the human mind. Computer memory is like your short-term memory, and the computer hard drive is like your long term memory. The more memory the computer has, the more things it can do at the same time. **You should get at least 8 GB of computer memory,** and consider getting 12GB or 16 GB for even better performance.

The hard drive is where the computer stores things that it needs to keep, such as documents, spreadsheets, pictures, programs, etc. The best decision is based on three things: Amount of storage needed, performance and cost. The choice is between a traditional hard drive or the new style SSD hard drive. Traditional hard drives use the same basic technology that has been around for over 40 years, but your storage capacity per dollar spent is very good. A SSD drive uses chips that are very similar to a computer's memory chips to store information and they are very fast. Because they are using newer technology and are faster the amount of storage per dollar spent is higher. In general, Traditional hard drives offer a lot of storage at a lower cost and SSD hard drives usually have less storage per dollar spent, but have much better performance. **If you want fast, then purchase the SSD drive. If you need to store a significant amount of files, then go with the traditional hard drive.**

Operating System
This is a source of great debate right now. Windows Microsoft currently supports versions 7, 8.1 and 10. **We recommend either Windows 7 or Windows 10, but make sure you purchase Professional version.** The home version does not have the same networking and security features and causes many support problems in a business environment.

Case Size
There are many sizes of computers today, from the big traditional tower sized computers down to the "tiny" cases that are about the size of router. The important thing to keep in mind is that as the case gets smaller there is less room for air to flow through the computer to keep it cool. The sources of heat are the power supply and the hard drive. If you are going with a smaller case like an Ultra Small Form Factor (USFF) or Tiny, make sure it has its power supply outside of the case. Many of these will use an outside power supply that looks like what you would use on a laptop. Another consideration is to get one with a SSD hard drive because they do not generate as much heat.

STAY AWAY FROM

All-In-One Computers
On the surface, the All-In-One computer concept sounds good. The power, processing and hard drive are all built into the same unit with the monitor. Having everything in one unit does save space. However, they tend to have heat related problems which may cause parts to not last as long. It is also more difficult to find parts and repair, which leads to higher costs more to maintain them. If you have a tight space to work with, there are better solutions.

Brands (other than Dell, HP or Lenovo)
For business use, it is best to stick with computers made by these three companies. Computers from these companies are easier to find parts for repairs, device drivers are readily available and they make quality products.

Windows 8
There is no compelling reason to run Windows 8, instead of Windows 7 or Windows 10. Both offer better performance, networking and usability as compared to Windows 8.

Home version of Windows
If you are using a computer for business, do not get the home version of Windows. The Home version of Windows does not have the security and networking features that are needed to function correctly in a business environment. This introduces security risks and creates support headaches that can be easily avoided by purchasing a computer with the Professional version of Windows installed.

Box Stores
Most "box" stores don't sell business quality computers. This includes Office Depot, Staples, Best Buy & Walmart. They all compete on lowest price (lowest quality) for technology and focus on consumer (home user) electronics. Their products tend to be computers that are either:

- lower quality product lines
- have less power
- Home versions of Windows
- Include junk programs, trials and advertising that are not needed on a business computer.

SOFTWARE & ACCESSORIES

When you start thinking about getting a new computer, you should also consider if you will need new software and accessories.

Office Software
These are the programs like Word, Excel, PowerPoint, Outlook and Publisher that are part of the Microsoft Office Suite. The choice now is between the traditional standalone version of Office 2016 (one time cost) Office 365 (recurring subscription). **We recommend Office 365 Business.** This gives you all of the programs in the Office Suite, each user can use Office on multiple devices and you get automatic upgrades so you do not have to worry about versions not working with one of your other users.

There are also free Office alternatives such as Google Docs, Libre Office and OpenOffice. However, these can be a more challenging to utilize and work with the macro files from HUD and with your housing or accounting software. Usually it is best to stay with Microsoft Office instead of one of the freebies.

Accounting Software
It is very common for housing authorities to also use an accounting program like Quickbooks for processing payroll, printing checks or managing collections. There are many accounting programs on the market today, but Quickbooks is the most universal and works well.

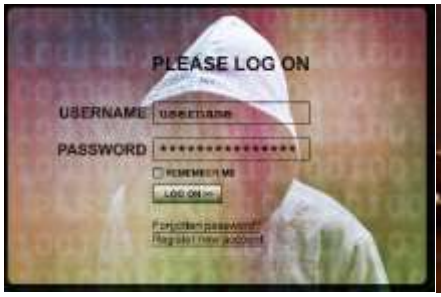
Monitors
Often, if your monitor is working fine, you might decide to continue using it. However, you might want to consider getting a new monitor or setting up dual monitors for your computer. Studies have shown a very good productivity increase from using 2 monitors.

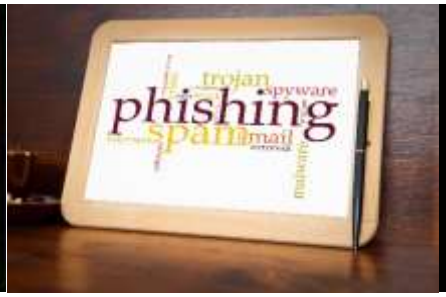
If you have a smaller monitor you might consider purchasing a larger monitor 24 or 27 Inch LED monitor. The price for larger monitors has decreased significantly over the last 2 years and larger monitors make it much easier to see everything on your screen if you have any kind of vision problem.

Let us help you find the right computer and equipment for your needs!
We also specialize in helping Housing Authorities!

UltimateITGuys.com

Be Safe Online – Don't Be A Victim





Avoiding Scams, Malware & Phishing

Scams, hacking, malware, viruses, & phishing are all about money. They are the actions of big business and are not just random things that happen to people. They are all parts of an illegal industry that makes a tremendous amount of money. They gather information through trickery, theft and data mining the information that we thoughtlessly place on the internet. The information is then held for ransom or sold to other criminals that use it to perform other illegal activities.

How do you avoid falling victim to scams, malware and phishing?

You start by setting up a solid defense against these threats, then you must be careful about the software that you install on your computers, how you use your computers and the information that you provide to others.

Solid Defense

For a solid defense, see our Standard Recommendations document for how to setup your computer and network to operate more securely.

Avoid downloading software that you don't want:

- **Download programs only from websites you trust.** If you are not sure whether to trust a program, enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware. Files that end in the extensions .exe or .scr commonly hide malware. However, even files with familiar extensions such as .docx, .xlsx, and .pdf can be dangerous.
- **Pay Attention & Read all security warnings, license agreements, and privacy statements** associated with any software you download. Before you install something, consider the risks and benefits of installing it. Even many reputable programs tell you that they are about to install additional software to "help" you, but it is usually software that you do not really need and often are programs that either spy on your behavior or lead to virus programs later.
- **Never click "Agree" or "OK" to close a window.** Instead, click the "x" in the corner of the window or press Alt + F4 on your keyboard to close a window.
- **Be Afraid of "free" things.** Such as "free" music and movie file-sharing programs, and be sure you understand all the software that is packaged with those programs.
- **Don't click links on suspicious websites or in email messages.** Instead, type the website address directly into your browser, or use bookmarks.
- **Don't automatically trust** that instant messages, email messages, or messages on social networking websites are from the person they appear to be from. Even if they are from someone you know, contact the person before you click the link to ensure that they intended to send it.
- **Ask someone who knows.** If you are not sure about a strange message or a program, then ask someone that you trust.

Email Safety

See our "Standard Recommendations" or "10 Email Safety Tips" documents for how to use your email more securely.

Computer Safety

See our Standard Recommendations document for suggestions on how to safely use your computer.

Mobile Safety

- Screen Lock Code
- Security App
- Mobile Device Management App
- Be careful about the information you provide when using your phone, tablet or laptop in a public setting. People can see what you are typing and hear what you are saying.

Phone Scams

- Most phone scammers are very high pressure and quite convincing. Do not give in to their tricks.
- Do not give personal or private information to someone who called you
- Do not give your credit card number to someone who called you
- Microsoft will not call you
- The IRS will not call you
- Be suspicious of anyone that calls you unexpectedly
- Random people do not call you to tell you that your computer is infected with a virus
- Do not give out passwords or other personal information over the phone
- If you have an error message with a phone number, do not call it
- If someone calls you, a good way to check them out is to call the main contact number on the company's website and ask for that person.
- Some of the questions that they ask may seem harmless like "do you shop online", "do you have any pets" or "how old are you", but these are classic phishing questions they use to gather more information about you and get you comfortable answering questions.

What To Do

Be paranoid. If something on your computer or the person on the phone doesn't seem right, then it probably isn't. Always verify before clicking a link, installing a program or giving out information.

If you think you have been hacked or have a virus, stop what you are doing and call your computer support person or someone who is knowledgeable about computer security immediately. The longer you use your computer after a virus or hack happens, the more difficult it is to remove the damage.

If you have given out your credit card number and are concerned about it, then call your credit card company to check your account and possibly put a fraud alert on the account. If there is already fraudulent activity on your card, then the best thing is to cancel the card and have a new one issued.

If you think one of your online accounts has been hacked, change the password and security questions. Verify what email accounts are allowed to reset the password. Sometimes hackers will insert their information into your account settings, so they will be notified of the password change or to block you from resetting the password.

If you need help or have questions about internet security, contact us using the information below.

UltimateITGuys.com

Standard Recommendations

Industry Best Practices For A Secure Computer

This is not an all-inclusive list, but it is a good place to start if you want to have a better, more secure computing experience. Following this set of recommendations will help to eliminate many of the headaches that effect most computer users.

General

1. Use a router based firewall to protect your network.
2. Use a good reputable full featured Anti-Virus/Malware program on all of your computers.
3. Password protect the Anti-virus software.
4. Have a proven & tested data Backup & Recovery plan.
5. Routinely clean your computer and remove any unnecessary programs.
6. Train your employees so they are aware of security threats & proper computer use.
7. Keep updates current for Windows, programs and security.
8. Don't install any software unless you are 100% sure you need it.
9. Use Business email accounts, not personal or freebie accounts.
10. When traveling do not use public or open unsecured wifi connections.

User

1. Users should operate under a "limited" account instead of "administrator" account.
2. Users don't install new programs and/or updates.
3. All computer user accounts have a good password.
4. File sharing is limited to a single shared folder on 1 computer and does not use the built in "Everyone" group.
5. Local documents are stored in the user's My Documents folder.
6. All shared documents are located on a shared drive with appropriate permissions for viewing and changing based on the User.
7. Do not use USB sticks for sharing files.
8. Don't install any software unless you are 100% sure you need it.
9. Don't let other people use your computer.
10. Don't open suspicious emails.
11. Don't share your private information.

.

Mobile

1. Physical Protection – Case & Screen Protector
2. Correct Charger
3. Screen Lock Code
4. Security App
5. Mobile Device Management App
6. Don't use Public "Open" wifi, such as at hotels & conference centers.

We are The Technology Service Provider for Housing Authorities!

Let Us Start Helping You!

What is the "Cloud" and is it safe?

The term "Cloud" is one of the most over used terms in the technology world today. It seems like every company is selling something that is "in the cloud", "uses the cloud", "is cloud ready", "cloud enabled".

You might hear the term Cloud in reference to the following service based products:

- Software As A Service(SaaS)
- Platform As A Service(Paas)
- Infrastructure As A Service(IaaS)

Usually, these cloud service products allow you to pay for actual usage or rent\pay by the month for the service, instead of buying the traditional software or hardware product. For example, Adobe Photoshop which can run several hundred dollars to purchase, but their SaaS offering is called Adobe Creative Cloud and lets you have the same functionality for as little as $9 per month.

You can also describe the cloud in terms of Private Cloud, Public Cloud or Hybrid Cloud, using the following definitions:

- **Private Cloud** is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.
- **Public Cloud** is when the services are rendered over a network that is open for public use and shares resources with many users or companies.
- **Hybrid Cloud** is a cloud computing service that is composed of some combination of private, and public cloud services, from different service providers.

Questions to ask about potential cloud service:

1. Will you use this cloud solution to work on or store sensitive information?
2. How fast is your network and Internet connection?
3. Do you need to access this information when outside of the office?
4. Where is the data physically stored?
5. Do you have multiple locations that need access to this information?
6. Do multiple users need access to this information?
7. Do you need to access this information across multiple types of devices, such as PC, laptop, tablet or phone?
8. What type of security and encryption does the service use?
9. What is the cloud provider's policy for data retention and destruction after cancellation of the service?
10. How often does the cloud provider create security updates, bug fixes or add new features?

Safety

The "Cloud" is not inherently good or bad in terms of safety. The best answer for you depends on how you answer the questions above. For most housing authorities, a hybrid or private cloud solution will work well, but there could be times when a public cloud service would make sense.

For most housing authorities, the need for a cloud solution normally involves

1. Sharing information between multiple users, devices or locations
2. Disaster Contingency Plan – Allowing you to conduct business if your primary location is unavailable because of fire, flood or other disaster.
3. Off-Site Storage of data for backup or archive purposes.
4. Housing Software that is web based or Software As A Service.

If you have questions or need help with a potential cloud project, feel free to contact us for help. We regularly provide private and hybrid cloud solutions for housing authorities. So we are familiar with the challenges that you face and the problems that you need to solve.

UltimateITGuys.com

How To Keep Your Computers Working

Basic Computer Maintenance

Basic Steps

1. Check your **backup**
2. Check for **updates to security** software
3. Check for **Virus and Malware activity**
4. Check **hard drive health** (run programs like Check Disk or the OEM Hardware diagnostics)
5. Check/remove **junkware programs & toolbars**
6. Clean **junk files** (temporary files, recycle bin, etc…)
7. Maintain your **hard drive** (run disk defrag on traditional hard drives, Trim on SSD drives)
8. Check for and install **Windows updates**
9. Check for and install **3rd party software updates** (Get the update from the manufacturer's website, not from a pop-up message)

These things are pretty straight forward, but the trick is:

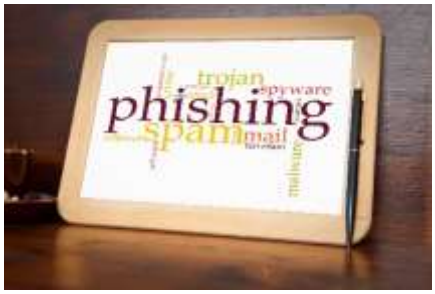
- Remembering to actually do the maintenance
- Performing the maintenance in the right order
- Knowing which updates are OK to install
- Knowing what to do when something bad shows up in the results
- Don't go download the latest thing that claims to do all of this for you. Most of these so called "cleaners" actually do more harm than good and some can even load viruses and malware on to your computer.
- Use reputable Anti-Virus such as Bit Defender, Kaspersky or Norton (No Free Stuff)
- Use a real backup program & test it periodically. Don't use freebie programs or USB drives.

Recommended Do It Yourself Tools

CCleaner - https://www.piriform.com/ccleaner/download
Smart Defrag - http://www.iobit.com/iobitsmartdefrag.html

Identity Theft

PROTECTING YOU, YOUR EMPLOYEES & YOUR RESIDENTS' INFORMATION



Why & How Does Identity Theft Happen?

When people think of identity theft, they picture their wallet getting stolen and someone using their driver's license and credit cards. However, with the Internet becoming increasingly important in our everyday lives, identify theft has moved online and into our computers and smart phones. Today viruses, phishing and identity theft are big businesses, often run by organized crime rings.

Identity theft is about information and money. It is the action of big business and not just random things that happen to people. Identity Theft, Hacking, Scams, Phishing, Viruses and Malware are all parts in an industry that makes a tremendous amount of money. These criminals gather information through trickery, theft and mining the information that you thoughtlessly place on the internet. The information is then held for ransom or sold to other criminals that use it to perform additional illegal activities.

Does Identity Theft Impact Housing Authorities?

As a Housing Authority you have been entrusted with **Personally Identifiable Information (PII)** from many people. You are responsible not only for your own information, but also the information of your co-workers, residents, and vendors. This is a serious responsibility.

You must take great care not to accidentally allow other people access to that data. Your actions might not seem significant at the time, but could turn into a big problem. If your computer gets infected with viruses or you fall prey to one of the many online phishing scams. By potentially opening up your user account or computer, you could create a huge problem for you and your housing authority.

What Should You Be Doing?

The best place to start any discussion about protecting information is with the user. You must use common sense, slow down and think about what you are doing instead of just clicking away with your mouse.

- Do you really need to install something?
- Does this email look or sound odd?
- Your personal actions can impact work.
- Passwords are a pain, but they do matter.
- Keeping your home PC virus free and protected matters.
- You are responsible and can be held liable if a data breach occurs.

Because many people reuse passwords between their personal and work accounts, what you do on your personal computer or devices when you are not at work is also important. If a hacker gets your information from one of your home accounts, they now may also have your information for your work account.

In today's connected world, many people work when they are at home. If you are working on a file at home on an infected computer and take it back to work, you can infect your work computer.

We see people all the time using personal email addresses at work and sharing so much information on Facebook that it is often a very simple exercise to guess their passwords or answers to security questions using this shared information.

To help protect yourself and those around you, you should be aware of online risks and the simple steps you can take against cyber threats. Below, are tips on how to stay safe in various environments.

Staying in Control

- **Connect securely wherever you are:** Only connect to the Internet over secure, password-protected networks. Never use public Wi-Fi in hotels or conference centers.
- **Think before you click:** Do not click on links or pop-ups, open attachments, or respond to emails from strangers.
- **Respond only to trusted messages:** Do not respond to online requests for personal information such as your date of birth or your credit card numbers; most organizations-banks, universities, companies, etc.-do not ask for your personal information over the internet.
- **Use passwords properly:** Select strong passwords and change them frequently. Password protect all devices that connect to the internet and user accounts.
- **Stay aware:** Routinely monitor bank and credit card accounts for unauthorized charges and unauthorized accounts that have been opened under your name.

Social Networks

- **Think before you post:** Limit the amount of personal information you post publicly. Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your friends post information about you, make sure the information is something that you are comfortable sharing with strangers.
- **Get smart and use privacy settings:** Take advantage of privacy and security settings. Use site settings to limit the information you share with the general public online.
- **Trust your gut:** Be wary of strangers and cautious of potentially misleading or false information.

Mobile Devices

- **Be aware across all your devices:** When using your mobile device use the same level of care you would on your computer.
- **Suspect links and texts:** Be suspicious of unknown links or requests sent through email or text message. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be, as some links are designed to gather your personal information.
- **Be careful what you download:** Download only trusted applications from reputable sources or marketplaces, as some apps may install harmful code onto your mobile device.
- **Anti-virus on-the-go:** Use a reputable full featured anti-virus program on your phone to perform routine checks.

At Home

- **Have a conversation with your family:** Talk to your family about Internet safety. Keep your family's computer in an open area and talk to your children about what they are doing online, including who they are talking to and what websites they are visiting.
- **Keep your computer clean and virus free:** It is more likely that something will happen to you on your home computer, because most people do not have proper security settings or anti-virus at home. Also, you tend to let your guard down when you are at home, so it is easier for hackers and scammers to get to you and your information. The problems from home can easily follow you to the office. If you use the same email at home and work or you take files home to work on them.

What To Do If Your Identity Has Been Stolen

- **First Steps**
  - **Place an Initial Fraud Alert** – Contact one of the three credit reporting bureaus: Experian, TransUnion, or Equifax to place a Fraud Alert.
  - **Order Your Credit Reports** – Order your credit reports from the credit reporting bureaus mentioned above,
  - **Create an Identity Theft Report** - You can file your report online, at the FTC website or by phone (toll-free): 1-877-ID THEFT (877-438-4338); TDD (toll-free): 1-866-653-4261, or by mail — 600 Pennsylvania Ave., Washington DC 20580.
- Next Steps
  - **Contact your credit card company:** Check each of your credit card accounts to see if you have fraudulent charges.
  - **Contact your bank, loans, credit and investment accounts**. – Check for fraudulent activity.
  - **Go to the Federal Trade Commission website for more information** at www.consumer.ftc.gov. A good article to check out is https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf

So You Want a Website

In today's world it seems like everything is on the internet. Everyone is telling you to get a website. So, should we build a website and put our business on the internet too? The advertisements say it is quick, easy and doesn't cost much. Well, here is the real story and some things to think about before you get started.

Some Things To Think About Before You Get Started

- Why do you want a website?
- What do you want it to do?
- Who is your audience?
- How will they find you?
- What is the Expected Outcome/Goal of the website?
- Who is going to create the content?

At the most basic level, your website needs to do at least 4 things:

1. Tell where to find you – Address, optionally directions and a map
2. Tell how to contact you – contact phone number & email, optionally a contact form
3. Tell What you do – In simple straight forward wording
4. Tell Who you are – A little about you and what sets you apart from everyone else

How well you do these 4 basic things will have a lot to do with the success of your website.

Let's move on to discussing the truth about how to make your website successful

TRUTH #1

Websites take money

There are many costs that if ignored will lead to a bad experience with your website

Examples: Costs for Design, Domain Name, Hosting, Backup, Updates / Upgrades, Content, Spam Filtering, Security

There are many costs involved in building and maintaining a successful website. Most people think that you build it and you are done. Nothing could be farther from the truth.

- You need to renew your domain name each year
- pay your hosting bill monthly or annually
- you should have backups of the site in case something goes wrong
- software updates need to be applied
- designs need to be changed to stay current
- content needs to be created & added
- your site needs to be protected from spam, malware and hackers

In summary, there is a lot to do and it takes money to do it.

Don't fall into the trap of the $5 website. You need a real website that is mobile ready and search engine friendly if you want people to use your website. The freebie or super cheap website builders do not produce a quality website that is ready to help your business achieve its goals. Spend the money on a web designer that can create a site that works with today's browsers and devices, is easy to add content and is optimized for the search engines like Google, Bing and Yahoo.

TRUTH #2

Websites take time (work)

Websites are work. Somebody has to create content and add that content to your website. This can be you or an employee, but it also could be an outside person or service that helps with some of the work if you don't have enough staff to handle it.

Another thing that is often overlooked are the maintenance items like backups, updates and security. These things take time or they can be outsourced, but rarely are they included in the cheaper web hosting plans.

TRUTH #3

Websites take continued focus

You will not have a very productive experience if all you do is throw some information on to your new website and never add or update anything again. It takes a commitment to update information and add new content if you want people to actually find and use your website.

TRUTH #4

The things that you do off-site matter just as much as your website

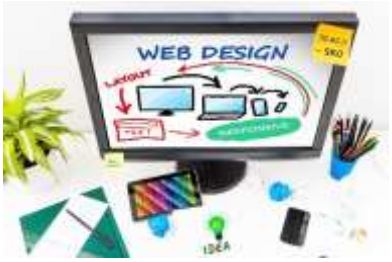
- All of your printed materials should point people to your website. Examples: business cards, letterhead, brochures, flyers.
- Make sure that information on other websites has the correct information about your business and points to your website. Examples: Google Places, Yahoo Local, Yellow Pages, Yelp, Etc…
- Train your employees to refer people to website.

TRUTH #5

Websites are not like the movie, Field of Dreams...Build it and they will come.

A better analogy for a website is probably "Jerry's World", AT&T Stadium in Dallas. People don't come to "see" Jerry's World, even though it is quite a sight. They come to see the events or what is happening at Jerry's world. It is the same with your website. Your website is just the venue to showcase your content and what is happening at your business. People go to websites that have useful, compelling, updated content and events.

If you build it correctly, put effort into providing valuable content and always point people to your website. This will encourage people to visit and utilize your website.



Quick Summary

Your website needs to do at least 4 things:

1. Tell where to find you – Address, optionally directions and a map
2. Tell how to contact you – contact phone number & email, optionally a contact form
3. Tell What you do – In simple straight forward wording
4. Tell Who you are – A little about you and what sets you apart from everyone else

The 3 biggest problems for websites are all based on commitment:

1. Money
2. Time
3. Focus

It takes money, time and focus to

- Create a website that is mobile and search friendly
- Create content
- Setup and maintain your off-site information
- Get people to your site
- Keep your site current

If you aren't willing to commit the needed money, time and focus to have a useable website, then your website is just a hobby.

If you need help with starting your website project or have more questions about websites, give us a call. We would be glad to help answer your questions.

You've Been Hacked!

Chances are high that you or your housing authority have been hacked. You probably do not realize it and you are potentially continuing to leak private information about you, your tenants, and your employees.

- **According to US government statistics, in 2016, the number of ransomware attacks increased 300 percent from 2015, with over 4,000 attacks detected per day.**
- **Most internet users can answer fewer than half the questions correctly on a knowledge quiz about cybersecurity issues and concepts. –** Pew Research Center
- **An 86% increase in Data Breaches in 2016 led to 1.4 Billion data records compromised…The leading type of breach is related to identity theft.**

Massive data breaches at companies like Yahoo and Target make headlines around the world. Yet the security threat does not just come from malicious outsiders. It very frequently comes from people within an organization who by accident or on purpose release sensitive information to unauthorized parties.

According to a recent study by BPI and FoxIT Software, there is "a glaring lack of effective security practices surrounding the way companies create and share confidential and sensitive documents. The result is that a wide range of high-value, confidential information is routinely at risk in businesses and government agencies today."

Study Highlights:

- Almost 75% of respondents say their organizations produce sensitive or confidential documents on a weekly or more frequent basis.
- Over 61% say their organizations lack effective document security.
- The number one document security challenge, by far, is accidently sending a confidential document to the wrong party.
- Close to 60% of people say they or someone they work with have mistakenly sent out documents they should not have.
- The vast majority of respondents believe increased connectivity and proliferation of devices have increased document security challenges in their organization.
- Respondents point to a wide range of repercussions for document leaks— from reputational damage and competitive risks, to lawsuits, lost revenue, lost time and job loss.
- 87% of senior managers admit to regularly uploading work files to a personal email or cloud account

Employees are often the weakest link in an organization. Hackers use social engineering to trick users into clicking on infected advertisements or URLs in emails or into downloading attachments that will infect the corporate network with ransomware.

Employees are the most common entry point for hackers seeking a way into your organization, so **regular security training** to educate them about network security and risk detection may reduce malware infections. Quite often the malicious code is implemented on legitimate websites to trick the untrained. The workers must learn to distinguish between authentic links, emails, and phishing scams

which could lead to viruses, ransomware infections or trick them into giving away passwords and sensitive information.

Multi-purpose devices used for both home and work tasks are a top risk. It only takes one random click to get infected. Once the device is connected to the company network, the infection can spread to the entire company network.

Hackers do not always need to expend much effort in breaching your network because you make it easy for them from the start. Many users do not have good passwords and often reuse their passwords. Using "free" email accounts puts your information at higher risk. Most small offices do not have proper business quality network equipment, security software and properly maintained computers. You should perform regular updates of all software, and check them for vulnerabilities. Most offices are not prepared and usually lack the skills to perform the routine maintenance, much less research and stay on top of these new threats.

Implement multiple prevention methods to lower the risks at your housing authority – it is always cheaper to prevent ransomware attacks, data losses and viruses than to spend money on recovering data and fixing problems afterward.

You need Business class tools; such as

- Business email with spam protection and real-time scanning of content
- Network equipment that protects everything on your network and monitors for unusual activity
- Security software that stops multiple types of threats and alerts when there is a problem
- Monitoring and management software that scans, updates and monitors for vulnerabilities on your computers
- A good solid backup plan

Remember your computers are tools, not toys. Housing Authorities are a business, treat your technology like business tools and take proper care of them. This will make your work safer and more productive.

Measure Your Security Risk

Answer Yes or No to the following questions. Yes=1 point, No=0 points

1. Do you use Yahoo or other "free"email?
2. Do you use USB sticks or flash drives?
3. Do you use hotel, coffee shop or other public wifi when travelling?
4. Do you let people connect to the wifi at your office?
5. Do you ever use your personal email for work?
6. You do not have a security training process.
7. Do you have a shared documents folder on one of your office computers?
8. Is your networking equipment limited to what your internet provider gave you?
9. Do you reuse the same password(s) on any of your online accounts?
10. Is your home page set to MSN, Yahoo or other "news" sites?

If you answered Yes to more than 3 of these questions you are at an increased risk of losing personal information related to your housing authority.

Ask about our Security Assessment Process. We remotely perform an assessment of your current computers and network then produce an action plan of what needs to be addressed.

UltimateITGuys.com

Free Email Could Cost You Everything!

How many of you have a “free” email address provided by your internet provider? Usually this means that you have an email address that ends in yahoo.com, sbcglobal.net, cox.net, comcast.net, pldi.net, etc…

That "Free" email account you are using could cost you everything you have.

Free email accounts are not secure!

1. When you use a free email, you are not the customer. The Email Provider makes money from advertisers and data miners who use your information to make more money off of you.

2. Advertisements in free email are a common source of viruses, malware and scams. This means that by just checking your email you are increasing your chances of getting a virus or being a victim of a scam.

3. Free email accounts do not provide good quality spam filtering. This means that you get a lot of junk mail. Often this junk mail contains viruses, it can also be a source of scams and attempts to gain access to your information by phishing.

4. Many of these free email providers have been hacked, sometimes repeatedly.

Yahoo announced that they had a breech which compromised information for over 500 million people. This information included names, email addresses, telephone numbers, dates of birth, security questions and answers, and in some cases passwords.

This is enough information to make it easy for someone to steal your identity, take over your other online accounts, reset your passwords and change other information about you with not just Yahoo, but other companies as well.

The implications for this breech and many others like it are very scary in today's online world, especially since most websites use your email as your User ID.
Because the bad guys have access to your email, they can reset your passwords with your other accounts and receive the password reset email.

All of this is further complicated by the fact that most people use the same password on many of their accounts. The combination of these 2 things makes it very easy for the bad guys to get access to most, if not all of your information very quickly.

They now have enough access to obtain credit, access your bank and retirement accounts, and generally make your life miserable.

We all really need to take our information and online account use more seriously.

The moral of this story is nothing in life is really free. There is always a cost. Don't use free email accounts, because free email could cost you everything.

If you have questions or would like to know more about business quality email, give us a call. We will be glad to help you.

Ultimate IT Guys specializes in helping Housing Authorities with their computers. We are the leading provider of full service support for the housing industry. We offer remote support, on-site support, off-site backup, anti-virus, preventative maintenance, website building and website hosting.

We are much more than a bunch of IT geeks that fix problems. We don't just sit around and wait for something to break. We are continually monitoring your environment and fixing many issues before they become problems. We are just a phone call away when you do have a question or need help. We meet with you regularly to make sure we understand your business needs and direction. This allows us to provide you with the best solutions and support. Our goal is to be a vital member of your team and make sure that your IT dollars are spent wisely. We want your technology experience to be stress free, secure, and productive.

We work with all major housing software vendors and are experienced at
dealing with HUD and housing specific issues.

Stop worrying about your

Technology,

Let Us Take Care of IT for You!

UltimateITGuys.com

Evaluating Mobile Solutions For Housing Authorities

The goal of this guide is to help you answer the following questions:

- Do I want to start a mobile project at my housing authority?
- Where do I begin?
- How do I begin?
- What questions do I need to ask make these decisions?

We are going to walk through a series of things that you need to consider before starting your project. There will be a lot of questions and thinking required, but we have tried to make it easier for you. There are a series of checklists and cheat sheets available on our website at www.UltiatelTGuys.com/mobile that accompany this guide on mobile solutions that will help you with the evaluation and planning processes.

Part 1 intro discusses to mobile solutions and Part 2 discusses taking care of your mobile investment.

Intro to Mobile Solutions

- Selecting your App
- Planning
- Training
- Follow the Process

Taking Care of Your Mobile Investment

- Physical Protection
- Security
- Mobile Device Management

SELECTING YOUR APP

Does the app meet your needs?

The first thing to consider when selecting your app is does the app meet your needs? Sometimes the right answer is simple, to get the app that is made by your housing software company. However, if it does not do everything you need then you will not be happy.

Does the app currently have all of the key features that are important to you? If not, what is missing and how important is this feature to the success of your project?

Does the app work with your existing software? If the app does not work with your housing software, then you are creating a problem. Example: If you are doing work orders, can the app get the tenant name, unit number, & phone number from your housing software. If not, then this will be a manual step to add this information each time. While this may not seem like a big problem on the surface, you want to minimize the amount of data entry that is required on the mobile device. Having to manually add information each time will frustrate the user and add unnecessary time to the work order process.

How much does it cost?

At some point, cost always enters into the decision making process. More expensive does not always mean better, but it also does not make sense to pay extra to get additional features if they are not needed.

Does it work with the device that you will be using? (Apple vs Android)

The debate over Apple vs Android can become quite heated. From a technology stand point, they both work well. Most people tend to be very passionate for one or the other. If most of the users already use Apple then it is a good idea to use Apple devices. If most of your users are Android users, then you probably should go with an Android device. Many projects fail because this was not properly handled.

What is the feature that you like most about this App?

What is the one feature about the app that stands out to you as the most helpful? Is it important to the success of your project? is it a critical “have to have” feature?

What is the thing that I dislike most about this App?

What is this app’s short coming? Is it important to the success of our project? In other words is it a critical “have to have” feature?

How good is the support?

Support is a key factor in the long term success of your project. Make sure there is a way to talk to a support person when you need them. Many companies have started implementing processes that require you to submit a ticket on their website, then they will call you at their convenience. This can be frustrating if you need. The quality of the answers or solutions they provide is another thing to immediately consider.

How often do they have updates?

Are they regularly releasing updates with new features and patches to security issues? Some companies just create the app and never touch it again. Stay away from companies that do not provide periodic updates. Be sure to question whether the price of updates or upgrades are included in your initial purchase price or if there will be additional charges for the updates.

What do other users say about it?

Talk to someone that already uses the app that you are considering getting. They can be a valuable source of information to help answer some of these questions. Be careful if they are giving a strongly negative evaluation of the app and ask some clarifying questions. Many times a strongly negative opinion of an app is based on one of the following causes that might not be the fault of the app:

- Lack of proper training
- Bad attitude about using the app
- They do not like the platform (Apple vs Android)

PLANNING

THINGS TO DO

- Document your process
- How & where will you use your mobile app
- Plan for the unexpected
  - Dead battery
  - No wifi signal
  - No cell service

PLANNING

Document your process

If you do not have a process for what, how and when you will use the app, you will get erratic results and end up frustrated with the app.

What, How & Where will you use your mobile app

Some considerations are:

- Do you have a good cellular and/or wifi signal at all of your locations? If cellular signal is poor, consider putting in a secured wifi router if possible.
- Will you be inputting information while you are inside or outside? Glare and visibility can be a problem with some devices in bright sunlight.
- Will you be sitting or standing while trying to enter information? If you are standing you should consider a case that has a loop for your hand on the back so you can hold on to the device while inputting information.
- When creating a work order, do you want to create a work order for every activity or will you have certain activities that are exceptions? 0

Plan for the unexpected

Planning for problems is critical to your success. It is helpful to everyone if they know what to do when there is a problem. Examples include:

- Who do you call if the app isn't working?
- If you do not have wifi or cell service in a building how can you get the information for your work order?
- If your phone or tablet is not working for some reason, what Is the procedure for completing the work order?

TRAINING

Training is critical to the success of your project. Train the users with the process that you have documented. Make sure that they know what to do when problems or surprises happen. Have a good contingency plan and make sure the users know what the contingency process is and when it is ok to use it.

If possible, use hands on training with real world scenarios to supplement the written training. This will give the user confidence and give you a chance to see that they know what to do when they are using it in the real world.

Your training will only be as good as the thought, time and effort that is put into it. Make sure that the users take it seriously and can demonstrate that they know what to do. Just reading through the document one time will not lead to good results.

We have all been through training where we said "yes, I think I've got it", but then on Monday when we try to do it we cannot remember what to do. Make sure that the users get plenty of chances to use the app while in training. This will help to reinforce what they read, give them a chance to get comfortable with the app and more chances to ask questions while there is still someone there to answer. This will help to ensure that they know what to do when they start using it for real. If possible, try to train in the morning then utilize it on the job in the afternoon. The shorter the time between the training and their first real world use the better your chance for success.

TRAINING

THINGS TO DO

- Train your users with the documented process
- Train your users on what to do when surprises happen
- Reinforce the written training with some hands on real world scenarios.

FOLLOW THE PROCESS

People, Process, & Technology. People are often the weakest link. your people are vital to the success of your project. It is human nature to get distracted and make simple mistakes. It is entirely different to have a bad attitude about the project or not be on board with seeing the project succeed. Sometimes the bad attitude of one person can doom the entire project if not dealt with quickly and decisively.

Everyone has to be accountable for their part in the process. As a manager or project leader you must be willing to hold everyone accountable to do their part and to have a good attitude about the project. This can be tough, especially at small housing authorities where all of the workers tend to have close ties to each other. If you are not willing to take a stand and hold each person accountable on the project, then you are in danger of the project failing. This is critical. Many projects fail even though they got all of the other steps correct, because they ignored this one.

FOLLOW THE PROCESS

THINGS TO CONSIDER

- People, Process, Technology. People are usually the weakest link
- Everyone has to be accountable for their part of the process.
- Following the process is critical. I have seen projects fail even though they got all of the other steps correct, but ignored this one.

SUMMARY

Just because there is a shiny new device or application out there, does not that it is a good thing for your business. Sometimes the best answer is No.

Use the steps outlined here to help make your decision to use mobile technology in your business.

Select the right app, plan & document how to use it, train your users, and make sure everyone follows the process. These are the keys to using mobile technology in your business.

LET US HELP YOU

If all of this sounds like a lot of work, it is. It takes a lot of time and research to stay on top of what is happening in the ever changing world of technology. At Ultimate IT Guys, we work with hundreds of computers every month. So we have a really good view into what is happening in the world of housing authority computers. This puts us into a unique position to help you with the computers at your housing authority. We have invested in the tools, hardware and software to help you keep your computers and network running their very best.

We want to be your IT Guys. Give us a call today, to let us start taking care of your computers.

VIP Managed Service Bundle includes

- Preventative Maintenance
- Anti-Virus
- Off-Site Backup
- Remote Support
- Business Email Service

Optional Services

- Office 365 Business or Enterprise
- Hosted Cloud Desktop
- Website Hosting and Maintenance
- Enhanced Backup Service – Total PC backup with recovery ability to another PC or Cloud
- Remote Access
- Enhanced Security Service – Includes
  - Full featured business security router
  - Network scanning
  - Web filtering
  - Application Control
  - Network Anti-Virus
  - Intrusion Protection
  - DNS Filtering
  - Cloud Access Security Inspection
  - Email scanning
  - Spam filtering
  - Email Archiving