ULTIMATE IT GUYS

UltimateITGuys.com

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

We are The Technology Service Provider for Housing Authorities!
Let Us Start Helping You!