

Crime Prevention Newsletter

Fort Worth, Texas

August 2007

Illegitimate Wireless Hotspots: Stealing Personal Information

Key Findings –

Illegitimate public wireless hotspots are being created using high-power, long-range wireless routers with ambiguous or apparently innocent names to trick unwitting users to log into the services.

Once a potential victim, typically using a laptop, has logged into the fraudulent wireless hotspots, personally identifiable information transmitted through the network, to include credit card information, bank account numbers, and login names and passwords, is collected and later used to make illegitimate purchases and fraudulent transfers of fund, and to steal identities.

Fraudulent wireless hotspots are likely at locations with large numbers of laptop users, such as airport waiting areas, hotel lobbies, coffee shops, and cafes.

Proliferation of Wireless Networks Provides Opportunities for Fraud –

The proliferation of wireless hotspots at public facilities is making it easier to connect to the Internet from any location. It is also becoming easier, however, for criminals to collect personal information transmitted by users believing they are connected to legitimate networks.

The growing number of free Internet wireless access points in public locations makes it difficult for a user to determine which are legitimate and which are not. The advent of high-power, long-range wireless routers has allowed criminals to establish fraudulent hotspots that cover wide areas where a large number of wireless Internet users congregate. Some common ploys that criminals use to disguise their activity include:

- Giving the fraudulent wireless hotspot the same (or similar) name as a legitimate wireless service provider, leading unsuspecting users to connect to the illegitimate hotspot instead of the legitimate one.
- Establishing wireless hotspots with innocuous or seemingly official names such as “Free Airport Wireless.”
- Using wireless routers programmed with default names (typically the name of the router manufacturer) and requiring no passwords to entice unsuspecting users.

Recommendations –

The Department of Homeland Security recommends caution when using publicly available wireless hotspots, balance convenience with personal information security considerations. Users should take the following precautions:

- Avoid using unfamiliar wireless hotspots.
- Avoid transmitting sensitive personal information such as e-mail logins, passwords, and credit card numbers when using public wireless hotspots.
- Register with a known wireless service provider when connected to a home or corporate network to avoid sending personal information over an unknown or unsecured network, and use only that wireless service provider.

Source: Department of Homeland Security, Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)



Report crimes, trespassers and suspicious activities to the ROCC at 800-832-5452.