

ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਹੈਂਡਬੁੱਕ

ਭਾਗ-2

ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਵੱਲ ਇੱਕ ਛੋਟਾ ਜਿਹਾ ਕਦਮ



ਰਾਜ ਵਿੱਦਿਅਕ ਖੋਜ ਅਤੇ ਸਿਖਲਾਈ ਪ੍ਰੀਸ਼ਦ, ਪੰਜਾਬ

ਤਿਆਰ ਕਰਤਾ: ਵਿਸ਼ਾਲ ਵਾਟਸ, ਕੰਪਿਊਟਰ ਫੈਕਲਟੀ, ਸ.ਸ.ਸ. ਕਰਨੀ ਖੇੜਾ (ਫਾਜ਼ਿਲਕਾ)

ਸੰਦੇਸ਼



ਪਿਆਰੇ ਵਿਦਿਆਰਥੀਓ,

ਅੱਜ ਦੇ ਤੇਜ਼ੀ ਨਾਲ ਬਦਲ ਰਹੇ ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ ਇੰਟਰਨੈੱਟ ਅਤੇ ਤਕਨਾਲੋਜੀ ਸਾਡੀ ਦਿਨਚਰੀਆ ਦਾ ਅਹਿਮ ਅੰਗ ਬਣ ਚੁੱਕੇ ਹਨ। ਇੱਕ ਵਿਦਿਆਰਥੀ ਵਜੋਂ ਤੁਸੀਂ ਆਨਲਾਈਨ ਸਿੱਖਿਆ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਵੱਖ-ਵੱਖ ਡਿਜਿਟਲ ਸਾਧਨਾਂ ਨਾਲ ਲਗਾਤਾਰ ਜੁੜੇ ਹੋਏ ਹੋ। ਇਸਦੇ ਨਾਲ-ਨਾਲ ਇਹ ਸਮਝਣਾ ਵੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਡਿਜਿਟਲ ਮਾਹੌਲ ਵਿੱਚ ਸੁਰੱਖਿਅਤ, ਸਚੇਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਢੰਗ ਨਾਲ ਵਰਤੋਂ ਕਰਨੀ ਕਿੰਨੀ ਮਹੱਤਵਪੂਰਨ ਹੈ।

ਸਾਈਬਰ ਹਮਲੇ, ਆਨਲਾਈਨ ਠੱਗੀਆਂ, ਸਾਈਬਰ ਬੁਲਿੰਗ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਚੋਰੀ ਵਰਗੀਆਂ ਚੁਣੌਤੀਆਂ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖਦੇ ਹੋਏ, ਪੰਜਾਬ ਰਾਜ ਵਿਦਿਅਕ ਖੋਜ ਅਤੇ ਸਿੱਖਲਾਈ ਪ੍ਰੀਸ਼ਦ, ਪੰਜਾਬ ਵੱਲੋਂ ਵਿਦਿਆਰਥੀਆਂ ਵਿੱਚ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਬਾਰੇ ਜਾਗਰੂਕਤਾ ਪੈਦਾ ਕਰਨ ਲਈ ਇਹ “ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਹੈਂਡਬੁੱਕ” ਤਿਆਰ ਕੀਤੀ ਗਈ ਹੈ। ਇਸ ਹੈਂਡਬੁੱਕ ਰਾਹੀਂ ਤੁਹਾਨੂੰ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣ, ਫਿਸ਼ਿੰਗ ਹਮਲਿਆਂ ਦੀ ਪਛਾਣ ਕਰਨ, ਸਾਈਬਰ ਨੈਤਿਕਤਾ (Cyber Ethics) ਅਤੇ ਆਨਲਾਈਨ ਗਤੀਵਿਧੀਆਂ ਦੌਰਾਨ ਅਪਣਾਈਆਂ ਜਾਣ ਵਾਲੀਆਂ ਸਾਵਧਾਨੀਆਂ ਬਾਰੇ ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਹੋਵੇਗੀ।

ਮੈਂ ਤੁਹਾਨੂੰ ਅਪੀਲ ਕਰਦੀ ਹਾਂ ਕਿ ਇਸ ਹੈਂਡਬੁੱਕ ਨੂੰ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹੋ, ਇਸ ਵਿੱਚ ਦਿੱਤੀ ਜਾਣਕਾਰੀ ਨੂੰ ਆਪਣੇ ਦੇਸ਼ਾਂ ਅਤੇ ਪਰਿਵਾਰ ਨਾਲ ਸਾਂਝੀ ਕਰੋ ਅਤੇ ਡਿਜਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਸਦਾ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ। ਯਾਦ ਰੱਖੋ, ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੋਈ ਵਿਕਲਪ ਨਹੀਂ ਸਗੋਂ ਸਾਡੀ ਸਾਂਝੀ ਅਤੇ ਲਾਜ਼ਮੀ ਜ਼ਿੰਮੇਵਾਰੀ ਹੈ। ਸਾਨੂੰ ਪੂਰਾ ਭਰੋਸਾ ਹੈ ਕਿ ਵਿਦਿਆਰਥੀ ਇਸ ਹੈਂਡਬੁੱਕ ਅਤੇ ਵਿਭਾਗ ਦੇ ਇਸ ਉਪਰਾਲੇ ਤੋਂ ਪੂਰਾ ਲਾਭ ਉਠਾਉਣਗੇ।

(ਕਿਰਨ ਸ਼ਰਮਾ, ਪੀ.ਸੀ.ਐਸ)

ਡਾਇਰੈਕਟਰ, ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ।

ਸੰਦੇਸ਼



ਪਿਆਰੇ ਵਿਦਿਆਰਥੀਓ,

ਮੈਨੂੰ ਇਹ ਜਾਣ ਕੇ ਬਹੁਤ ਖੁਸ਼ੀ ਹੋ ਰਹੀ ਹੈ ਕਿ ਵਿਦਿਆਰਥੀਆਂ ਵਿੱਚ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਪ੍ਰਤੀ ਜਾਗਰੂਕਤਾ ਵਧਾਉਣ ਲਈ ਇਹ ਹੈਂਡਬੁੱਕ ਤਿਆਰ ਕੀਤੀ ਗਈ ਹੈ। ਅੱਜ ਦੇ ਆਧੁਨਿਕ ਡਿਜ਼ਿਟਲ ਯੁੱਗ ਵਿੱਚ ਇੰਟਰਨੈੱਟ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਸਾਡੀ ਦਿਨਚਰੀ ਦਾ ਅਟੂਟ ਹਿੱਸਾ ਬਣ ਚੁੱਕੇ ਹਨ, ਪਰ ਇਨ੍ਹਾਂ ਦੀ ਸਹੀ, ਸੋਚ-ਵਿਚਾਰ ਨਾਲ ਕੀਤੀ ਵਰਤੋਂ ਅਤੇ ਸੁਰੱਖਿਆ ਪ੍ਰਤੀ ਸਚੇਤਤਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

“ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਹੈਂਡਬੁੱਕ” ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਆਨਲਾਈਨ ਸੰਸਾਰ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਢੰਗ ਨਾਲ ਵਰਤੋਂ ਕਰਨ ਲਈ ਮਾਰਗਦਰਸ਼ਨ ਪ੍ਰਦਾਨ ਕਰਦੀ ਹੈ। ਇਸ ਵਿੱਚ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣ, ਡਾਟਾ ਗੋਪਨੀਯਤਾ, ਆਨਲਾਈਨ ਧੋਖਾਧੜੀਆਂ, ਹੈਕਿੰਗ ਅਤੇ ਸਾਈਬਰ ਬੁਲਿੰਗ ਵਰਗੀਆਂ ਮਹੱਤਵਪੂਰਨ ਚੁਣੌਤੀਆਂ ਬਾਰੇ ਵਿਸਥਾਰ ਨਾਲ ਜਾਣਕਾਰੀ ਦਿੱਤੀ ਗਈ ਹੈ। ਕਿਉਂਕਿ ਸਾਈਬਰ ਅਪਰਾਧੀ ਨਿੱਤ ਨਵੇਂ ਤਰੀਕਿਆਂ ਨਾਲ ਲੋਕਾਂ ਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾਉਂਦੇ ਹਨ, ਇਸ ਲਈ ਸਾਵਧਾਨ ਰਹਿਣਾ ਅਤੇ ਉਚਿਤ ਸੁਰੱਖਿਆ ਉਪਾਅ ਅਪਣਾਉਣਾ ਅਤਿ-ਆਵਸ਼ਕ ਹੈ।

ਮੈਂ ਸਾਰੇ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਅਪੀਲ ਕਰਦਾ ਹਾਂ ਕਿ ਇਸ ਹੈਂਡਬੁੱਕ ਵਿੱਚ ਸ਼ਾਮਲ ਹਰ ਵਿਸ਼ੇ ਨੂੰ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹਣ ਅਤੇ ਇਸ ਵਿੱਚ ਦਿੱਤੇ ਗਏ ਸੁਝਾਵਾਂ ਨੂੰ ਆਪਣੀ ਰੋਜ਼ਾਨਾ ਦੀਆਂ ਆਨਲਾਈਨ ਗਤੀਵਿਧੀਆਂ ਵਿੱਚ ਅਮਲ ਵਿੱਚ ਲਿਆ ਕੇ ਆਪਣੇ ਆਪ ਨੂੰ ਅਤੇ ਹੋਰਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ।

(ਰਾਜੀਵ ਕੁਮਾਰ)

ਸਹਾਇਕ ਡਾਇਰੈਕਟਰ (AQT)

ਦਫ: ਡਾਇਰੈਕਟਰ ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ

ਸੰਦੇਸ਼



ਪਿਆਰੇ ਵਿਦਿਆਰਥੀਓ,

ਅਸੀਂ ਅੱਜ ਇੱਕ ਅਜਿਹੇ ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ ਜੀ ਰਹੇ ਹਾਂ ਜਿੱਥੇ ਇੰਟਰਨੈਟ ਸਿੱਖਿਆ, ਮਨੋਰੰਜਨ ਅਤੇ ਰੋਜ਼ਾਨਾ ਜੀਵਨ ਦਾ ਅਟੂਟ ਅੰਗ ਬਣ ਚੁੱਕਾ ਹੈ। ਤਕਨਾਲੋਜੀ ਨੇ ਜਿੱਥੇ ਸਾਡਾ ਜੀਵਨ ਸੁਖਾਲਾ ਬਣਾਇਆ ਹੈ, ਉੱਥੇ ਹੀ ਇਸ ਨਾਲ ਜੁੜੇ ਕਈ ਨਵੇਂ ਖਤਰੇ ਵੀ ਸਾਹਮਣੇ ਆਏ ਹਨ। ਸਾਈਬਰ ਅਪਰਾਧ, ਆਨਲਾਈਨ ਠੱਗੀਆਂ, ਸਾਈਬਰ ਬੁਲਿੰਗ, ਨਿੱਜੀ ਡਾਟਾ ਚੋਰੀ ਅਤੇ ਭ੍ਰਮਕ ਖ਼ਬਰਾਂ ਵਰਗੀਆਂ ਚੁਣੌਤੀਆਂ ਤੋਂ ਸਚੇਤ ਰਹਿਣਾ ਅੱਜ ਦੇ ਸਮੇਂ ਦੀ ਮਹੱਤਵਪੂਰਨ ਲੋੜ ਹੈ।

ਡਿਜਿਟਲ ਸੰਸਾਰ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਨਾਗਰਿਕ ਬਣਨ ਲਈ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੇ ਮੂਲ ਨਿਯਮਾਂ ਦੀ ਸਮਝ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਮਜ਼ਬੂਤ ਅਤੇ ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਬਣਾਉਣਾ, ਅਣਜਾਣ ਲਿੰਕਾਂ ਜਾਂ ਸੁਨੇਹਿਆਂ ਤੋਂ ਬਚਣਾ, ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸੋਚ-ਵਿਚਾਰ ਨਾਲ ਸਾਂਝੀ ਕਰਨਾ ਅਤੇ ਇੰਟਰਨੈਟ ਉੱਤੇ ਸੁਰੱਖਿਅਤ ਆਚਰਨ ਅਪਣਾਉਣਾ ਹਰ ਵਿਦਿਆਰਥੀ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਹੈ।

“ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਹੈੱਡਬੁੱਕ” ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਇੱਕ ਭਰੋਸੇਮੰਦ ਰਹਿਨੁਮਾ ਹੈ, ਜੋ ਤੁਹਾਨੂੰ ਆਨਲਾਈਨ ਜਗਤ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਲੋੜੀਂਦੀ ਜਾਣਕਾਰੀ, ਸਮਝ ਅਤੇ ਯੋਗਤਾ ਪ੍ਰਦਾਨ ਕਰੇਗਾ। ਮੈਂ ਤੁਹਾਨੂੰ ਅਪੀਲ ਕਰਦਾ ਹਾਂ ਕਿ ਇਸ ਹੈੱਡਬੁੱਕ ਨੂੰ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹੋ, ਇਸ ਵਿੱਚ ਦਿੱਤੇ ਸੁਝਾਵਾਂ ਨੂੰ ਅਮਲ ਵਿੱਚ ਲਿਆਓ ਅਤੇ ਇਸਨੂੰ ਆਪਣੇ ਦੋਸਤਾਂ ਅਤੇ ਪਰਿਵਾਰ ਨਾਲ ਵੀ ਸਾਂਝਾ ਕਰੋ ਤਾਂ ਜੋ ਸੁਰੱਖਿਅਤ ਡਿਜਿਟਲ ਸਮਾਜ ਦੀ ਰਚਨਾ ਕੀਤੀ ਜਾ ਸਕੇ।

ਆਉ, ਅਸੀਂ ਮਿਲ ਕੇ ਇੱਕ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜਿਟਲ ਭਵਿੱਖ ਵੱਲ ਵਧੀਏ।

(ਸੰਦੀਪ ਯਾਦਵ)

ਸਟੇਟ ਪ੍ਰੋਜੈਕਟ ਕੋਆਰਡੀਨੇਟਰ (ਕੰਪਿਊਟਰ ਸਾਇੰਸ)

ਦਫ਼: ਡਾਇਰੈਕਟਰ ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ

ਸੰਦੇਸ਼



ਸਤਿਕਾਰਯੋਗ ਡਾਇਰੈਕਟਰ ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ ਸ਼੍ਰੀਮਤੀ ਕਿਰਨ ਸ਼ਰਮਾ (ਪੀ.ਸੀ.ਐਸ.), ਸ੍ਰੀ ਰਾਜੀਵ ਕੁਮਾਰ, ਸਹਾਇਕ ਡਾਇਰੈਕਟਰ (AQT), ਦਫ਼ਤਰ ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ ਜੀ ਦੀ ਯੋਗ ਅਗਵਾਈ ਅਤੇ ਸ਼੍ਰੀ ਸੰਦੀਪ ਯਾਦਵ, ਸਟੇਟ ਪ੍ਰੋਜੈਕਟਰ ਕੋਆਰਡੀਨੇਟਰ (ਕੰਪਿਊਟਰ ਸਾਇੰਸ), ਦਫ਼ਤਰ ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ ਦੀਆਂ ਕੀਮਤੀ ਹਦਾਇਤਾਂ ਦੇ ਸਦਕਾ, ਮੇਰੇ ਵੱਲੋਂ ਪੰਜਾਬ ਰਾਜ ਦੇ ਸਰਕਾਰੀ ਸਕੂਲਾਂ ਦੇ ਵਿਦਿਆਰਥੀਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਅਤੇ ਇੰਟਰਨੈਟ ਦੀ ਪਾਠਕ੍ਰਮਿਕ ਵਰਤੋਂ ਨੂੰ ਹੋਰ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਬਣਾਉਣ ਲਈ “ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਹੈਂਡਬੁੱਕ (ਭਾਗ-2)” ਤਿਆਰ ਕਰਨ ਦਾ ਇੱਕ ਨਿਮਰ ਉਪਰਾਲਾ ਕੀਤਾ ਗਿਆ ਹੈ।

ਇਸ ਹੈਂਡਬੁੱਕ ਵਿੱਚ ਮੌਜੂਦਾ ਸਮੇਂ ਦੀਆਂ ਲੋੜਾਂ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖਦੇ ਹੋਏ ਉਹ ਸਾਰੇ ਮਹੱਤਵਪੂਰਨ ਵਿਸ਼ੇ ਸ਼ਾਮਲ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕੀਤੀ ਗਈ ਹੈ, ਜੋ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਸਾਈਬਰ ਸੰਸਾਰ ਵਿੱਚ ਸਚੇਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਬਣਨ ਦੇ ਨਾਲ-ਨਾਲ ਇੰਟਰਨੈਟ ਦੀ ਸੁਚੱਜੀ ਅਤੇ ਸੁਰੱਖਿਅਤ ਵਰਤੋਂ ਰਾਹੀਂ ਵੱਧ ਤੋਂ ਵੱਧ ਲਾਭ ਪ੍ਰਾਪਤ ਕਰਨ ਵਿੱਚ ਸਹਾਇਕ ਸਾਬਤ ਹੋਣਗੇ।

ਆਸ ਕਰਦਾ ਹਾਂ ਕਿ ਇਹ ਹੈਂਡਬੁੱਕ ਆਪ ਸਭ ਨੂੰ ਇੰਟਰਨੈਟ ਦੀ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਤ ਤਰੀਕਿਆਂ ਨਾਲ ਅੱਗੇ ਵਧਣ ਵਿੱਚ ਮਦਦ ਕਰੇਗੀ।

ਵਿਸ਼ਾਲ ਵਾਟਸ (ਕੰਪਿਊਟਰ ਫੈਕਲਟੀ)
(ਹੈਂਡਬੁੱਕ ਤਿਆਰ ਕਰਤਾ)
ਸਸਸਸ ਕਰਨੀਖੇੜਾ, ਜਿਲ੍ਹਾ ਫਾਜ਼ਿਲਕਾ

ਪ੍ਰੇਰਨਾ ਸਰੋਤ
ਸ਼੍ਰੀਮਤੀ ਮੰਜੂ ਠਕਰਾਲ (ਪ੍ਰਿੰਸੀਪਲ)
ਸਸਸ ਕਰਨੀਖੇੜਾ ਜਿਲ੍ਹਾ ਫਾਜ਼ਿਲਕਾ

ਸੋਧ ਕਰਤਾ
ਸ਼੍ਰੀਮਤੀ ਅਦਿਤੀ (ਪੰਜਾਬੀ ਮਿਸਟ੍ਰੈਸ)
ਸਸਸ ਲਾਲੇ ਵਾਲੀ ਜਿਲ੍ਹਾ ਫਾਜ਼ਿਲਕਾ

ਵਿਸ਼ੇਸ਼ ਧੰਨਵਾਦ
ਸ਼੍ਰੀ ਸੰਦੀਪ ਯਾਦਵ (ਸਟੇਟ ਪ੍ਰੋਜੈਕਟ ਕੋਆਰਡੀਨੇਟਰ, ਕੰਪਿਊਟਰ ਸਾਇੰਸ)
ਦਫ਼ਤਰ ਐਸ.ਸੀ.ਈ.ਆਰ.ਟੀ. ਪੰਜਾਬ

ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਸਬੰਧੀ ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਹੈਂਡਬੁੱਕ ਭਾਗ-2

ਤਿਆਰ ਕਰਤਾ:
ਵਿਸ਼ਾਲ ਵਾਟਸ (ਕੰਪਿਊਟਰ ਫੈਕਲਟੀ)
ਸਸਸਸ ਕਰਨੀਖੇੜਾ (ਫਾਜ਼ਿਲਕਾ)

ਹੈਂਡਬੁੱਕ ਵਿੱਚ ਕਵਰ ਕੀਤੇ ਗਏ ਟੋਪਿਕ

1. ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਬੁਨਿਆਦੀ ਜਾਣਕਾਰੀ
2. ਮਜ਼ਬੂਤ ਅਤੇ ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਬਾਰੇ ਜਾਣਕਾਰੀ
3. ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਸੁਰੱਖਿਅਤ ਵਰਤੋਂ ਸਬੰਧੀ ਸੁਝਾਅ
4. ਸਾਈਬਰ ਬੁੱਲਿੰਗ (Cyberbullying) ਅਤੇ ਇਸ ਤੋਂ ਬਚਾਵ ਦੇ ਤਰੀਕੇ
5. ਫਿਸ਼ਿੰਗ ਠੱਗੀ ਕੀ ਹੈ? ਇਸ ਤੋਂ ਬਚਾਅ ਦੇ ਤਰੀਕੇ
6. ਵਿਦਿਆਰਥੀਆਂ ਵਿੱਚ ਆਨਲਾਈਨ ਗੇਮਾਂ ਖੇਡਣ ਦੀ ਆਦਤ ਅਤੇ ਇਸ ਸਬੰਧੀ ਸੁਝਾਅ
7. ਡਿਜ਼ੀਟਲ ਐਟਿਕੇਟ ਦਾ ਮਤਲਬ ਅਤੇ ਇਸ ਦੀ ਜਰੂਰਤ
8. ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਸਬੰਧੀ ਜਰੂਰੀ ਸੁਝਾਅ
9. ਮੋਬਾਈਲ ਫੋਨ ਸੁਰੱਖਿਆ ਬਾਰੇ ਜਾਣਕਾਰੀ
10. ਜਾਣੇ ਅਣਜਾਣੇ ਵਿੱਚ ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਗਲਤ ਜਾਣਕਾਰੀ ਸਾਂਝਾ ਕਰਨ ਸਬੰਧੀ ਜਾਗਰੂਕਤਾ
11. ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਅਤੇ ਕਾਨੂੰਨੀ ਜਾਣਕਾਰੀ
12. ਆਮ ਤੌਰ ਤੇ ਵਰਤੇ ਜਾਣ ਵਾਲੇ ਡਿਜ਼ੀਟਲ ਡਿਵਾਇਸਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਤਰੀਕੇ ਨਾਲ ਵਰਤਣ ਸਬੰਧੀ ਸੁਝਾਅ
13. ਆਨਲਾਈਨ ਕਲਾਸਾਂ ਅਤੇ ਈ-ਲਰਨਿੰਗ ਸੁਰੱਖਿਆ ਸਬੰਧੀ ਹਦਾਇਤਾਂ
14. ਆਨਲਾਈਨ ਸਿੱਖਣ ਅਤੇ ਡਿਜ਼ੀਟਲ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਸਬੰਧੀ ਮਾਪਿਆਂ ਦੀ ਭੂਮਿਕਾ
15. ਐਮਰਜੈਂਸੀ ਸਥਿਤੀਆਂ
16. ਭਾਰਤ ਸਰਕਾਰ ਦੇ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਸ਼ਿਕਾਇਤ ਪੋਰਟਲ ਤੇ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਵਾਉਣ ਦਾ ਤਰੀਕਾ
17. ਆਨਲਾਈਨ ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ ਬਾਰੇ ਜਾਣਕਾਰੀ
18. ਭਾਰਤ ਸਰਕਾਰ ਦੀ ਸੰਚਾਰ ਸਾਥੀ ਐਪ ਸੰਬੰਧੀ ਸੰਪੂਰਨ ਜਾਣਕਾਰੀ
19. ਆਪਣਾ ਮੋਬਾਈਲ ਫੋਨ ਹੈਕਿੰਗ ਤੋਂ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਰੱਖੀਏ
20. ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦਾ ਪ੍ਰਣ

1. ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਬੁਨਿਆਦੀ ਜਾਣਕਾਰੀ

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕੀ ਹੈ?

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਉਹ ਪ੍ਰਕਿਰਿਆ ਅਤੇ ਤਕਨੀਕਾਂ ਦਾ ਸਮੂਹ ਹੈ ਜੋ ਕੰਪਿਊਟਰਾਂ, ਮੋਬਾਈਲਾਂ, ਨੈੱਟਵਰਕਾਂ, ਸਰਵਰਾਂ ਅਤੇ ਡਿਜ਼ਿਟਲ ਡਾਟਾ ਨੂੰ ਗੈਰ-ਅਧਿਕਾਰਿਤ ਪਹੁੰਚ, ਹਮਲਿਆਂ, ਨੁਕਸਾਨ ਜਾਂ ਚੋਰੀ ਤੋਂ ਬਚਾਉਂਦਾ ਹੈ। ਜਿਵੇਂ-ਜਿਵੇਂ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਵਧ ਰਹੀ ਹੈ, ਉਸੇ ਤਰ੍ਹਾਂ ਸਾਈਬਰ ਹਮਲਿਆਂ ਦੇ ਖਤਰੇ ਵੀ ਵਧ ਰਹੇ ਹਨ—ਉਦਾਹਰਨ ਲਈ ਹੈਕਿੰਗ, ਮਾਲਵੇਅਰ, ਫਿਸ਼ਿੰਗ, ਰੈਂਸਮਵੇਅਰ, ਡਾਟਾ ਲੀਕ ਆਦਿ। ਇਨ੍ਹਾਂ ਹਮਲਿਆਂ ਤੋਂ ਬਚਾਅ ਲਈ ਜ਼ਰੂਰੀ ਸੁਰੱਖਿਆ ਪ੍ਰਬੰਧਾਂ ਨੂੰ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਕਿਹਾ ਜਾਂਦਾ ਹੈ।

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਵਿੱਚ ਕਈ ਤਰ੍ਹਾਂ ਦੀਆਂ ਵਿਧੀਆਂ ਵਰਤੀਆਂ ਜਾਂਦੀਆਂ ਹਨ, ਜਿਵੇਂ ਕਿ ਫਾਇਰਵਾਲ, ਐਂਟੀ-ਵਾਇਰਸ, ਐਨਕ੍ਰਿਪਸ਼ਨ, ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA), ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ, ਅਤੇ ਨਿਯਮਿਤ ਸਾਫਟਵੇਅਰ ਅਪਡੇਟ। ਇਹ ਸਾਰੇ ਤਰੀਕੇ ਡਾਟਾ ਨੂੰ ਬਾਹਰੀ ਖ਼ਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਮਦਦ ਕਰਦੇ ਹਨ।

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਲੋੜ ਸਿਰਫ਼ ਵੱਡੀਆਂ ਕੰਪਨੀਆਂ ਨੂੰ ਹੀ ਨਹੀਂ, ਸਗੋਂ ਆਮ ਲੋਕਾਂ ਨੂੰ ਵੀ ਹੈ। ਅਸੀਂ ਆਪਣੇ ਮੋਬਾਈਲ ਫੋਨਾਂ 'ਤੇ ਬੈਂਕਿੰਗ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਖਰੀਦਦਾਰੀ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਰੱਖਦੇ ਹਾਂ। ਜੇ ਇਹ ਜਾਣਕਾਰੀ ਗਲਤ ਹੱਥਾਂ ਵਿੱਚ ਚਲੀ ਜਾਵੇ ਤਾਂ ਆਰਥਿਕ ਨੁਕਸਾਨ, ਪਹਿਚਾਣ ਦੀ ਚੋਰੀ ਅਤੇ ਹੋਰ ਕਈ ਮੁਸ਼ੀਬਤਾਂ ਆ ਸਕਦੀਆਂ ਹਨ। ਇਸ ਲਈ ਹਰ ਕਿਸੇ ਨੂੰ ਬੁਨਿਆਦੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੇ ਨਿਯਮਾਂ ਦੀ ਪਾਲਣਾ ਕਰਨੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।



ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦਾ ਇੱਕ ਹੋਰ ਮਹੱਤਵਪੂਰਨ ਪੱਖ ਹੈ ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ। ਲੋਕਾਂ ਨੂੰ ਇਹ ਪਤਾ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਕਿਹੜੀਆਂ ਲਿੰਕਾਂ ‘ਤੇ ਕਲਿੱਕ ਨਹੀਂ ਕਰਨਾ, ਕਿਹੜੇ ਸੁਨੇਹੇ ਫਰਜ਼ੀ ਹੋ ਸਕਦੇ ਹਨ ਅਤੇ ਕਿਵੇਂ ਆਪਣੇ ਡਾਟਾ ਦੀ ਸੁਰੱਖਿਆ ਕਰਨੀ ਹੈ।

ਇੰਟਰਨੈੱਟ ਕੀ ਹੈ?

ਇੰਟਰਨੈੱਟ ਦੁਨੀਆ ਭਰ ਦੇ ਕਰੋੜਾਂ ਕੰਪਿਊਟਰਾਂ, ਮੋਬਾਈਲ ਫੋਨਾਂ, ਸਰਵਰਾਂ ਅਤੇ ਹੋਰ ਡਿਜ਼ੀਟਲ ਡਿਵਾਈਸਾਂ ਨੂੰ ਆਪਸ ਵਿੱਚ ਜੋੜਨ ਵਾਲਾ ਇੱਕ ਵੱਡਾ ਗਲੋਬਲ ਨੈੱਟਵਰਕ ਹੈ। ਇਸ ਦੇ ਜ਼ਰੀਏ ਜਾਣਕਾਰੀ ਨੂੰ ਇੱਕ ਜਗ੍ਹਾ ਤੋਂ ਦੂਜੀ ਜਗ੍ਹਾ ਤੱਕ ਸਕਿੰਟਾਂ ਵਿੱਚ ਭੇਜਿਆ ਜਾ ਸਕਦਾ ਹੈ। ਇੰਟਰਨੈੱਟ ਨੂੰ ਅਕਸਰ “ਜਾਲ” ਕਿਹਾ ਜਾਂਦਾ ਹੈ ਕਿਉਂਕਿ ਇਹ ਕਈ ਛੋਟੇ ਨੈੱਟਵਰਕਾਂ ਨੂੰ ਮਿਲਾ ਕੇ ਬਣਿਆ ਹੈ।

ਇੰਟਰਨੈੱਟ ਦੀ ਸ਼ੁਰੂਆਤ 1960 ਦੇ ਦਹਾਕੇ ਵਿੱਚ ਅਮਰੀਕਾ ਦੀ ARPANET ਪ੍ਰੋਜੈਕਟ ਨਾਲ ਹੋਈ ਸੀ, ਪਰ ਸਮੇਂ ਦੇ ਨਾਲ ਇਹ ਵਧਦਾ ਗਿਆ ਅਤੇ ਅੱਜ ਨਿੱਜੀ, ਵਪਾਰਕ, ਸਰਕਾਰੀ ਅਤੇ ਸਿੱਖਿਆ ਸੰਬੰਧੀ ਲੱਖਾਂ ਨੈੱਟਵਰਕ ਇਸ ਨਾਲ ਜੁੜੇ ਹਨ। ਇੰਟਰਨੈੱਟ ਦੇ ਕੰਮ ਕਰਨ ਦਾ ਧਾਰਾ TCP/IP (Transmission Control Protocol / Internet Protocol) ‘ਤੇ ਆਧਾਰਿਤ ਹੈ, ਜੋ ਡਾਟਾ ਨੂੰ ਛੋਟੇ-ਛੋਟੇ ਹਿੱਸਿਆਂ ਵਿੱਚ ਤੋੜ ਕੇ ਸਹੀ ਮੰਜ਼ਿਲ ਤੱਕ ਪਹੁੰਚਾਉਂਦਾ ਹੈ।

ਇੰਟਰਨੈੱਟ ਰਾਹੀਂ ਅਸੀਂ ਬਹੁਤ ਸਾਰੀਆਂ ਸੇਵਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹਾਂ, ਜਿਵੇਂ ਕਿ **ਵੈਬਸਾਈਟਾਂ (WWW)**, **ਈਮੇਲ**, **ਸੋਸ਼ਲ ਮੀਡੀਆ**, **ਵੀਡੀਓ ਕਾਲਾਂ**, **ਆਨਲਾਈਨ ਖਰੀਦਦਾਰੀ**, **ਆਨਲਾਈਨ ਬੈਂਕਿੰਗ**, ਆਦਿ। ਅੱਜ ਦੇ ਯੁੱਗ ਵਿੱਚ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰਨ, ਮਨੋਰੰਜਨ, ਬਿਜ਼ਨਸ ਚਲਾਉਣ, ਸਿੱਖਿਆ ਪ੍ਰਾਪਤ ਕਰਨ ਅਤੇ ਦੁਨੀਆਂ ਨਾਲ ਜੁੜੇ ਰਹਿਣ ਲਈ ਇੰਟਰਨੈੱਟ ਇੱਕ ਬੁਨਿਆਦੀ ਜ਼ਰੂਰਤ ਬਣ ਚੁੱਕਾ ਹੈ।

ਇੰਟਰਨੈੱਟ ਦੇ ਫਾਇਦਿਆਂ ਦੇ ਨਾਲ ਕੁਝ ਚੁਣੌਤੀਆਂ ਵੀ ਹਨ, ਜਿਵੇਂ ਕਿ **ਸਾਈਬਰ ਸੁਰੱਖਿਆ**, **ਫੇਕ ਨਿਊਜ਼**, **ਡਾਟਾ ਚੋਰੀ** ਆਦਿ। ਪਰ ਸਹੀ ਸਾਵਧਾਨੀਆਂ ਨਾਲ ਇੰਟਰਨੈੱਟ ਮਨੁੱਖਤਾ ਲਈ ਇੱਕ ਬਹੁਤ ਤਾਕਤਵਰ ਅਤੇ ਲਾਹੇਵੰਦ ਸਾਧਨ ਹੈ। ਇਸ ਨੇ ਦੁਨੀਆਂ ਨੂੰ ਇੱਕ “ਗਲੋਬਲ ਗਾਂਥ” ਵਾਂਗ ਜੋੜ ਦਿੱਤਾ ਹੈ।

ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਕੀ ਹੁੰਦਾ ਹੈ?

ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਉਹ ਸਾਰੇ ਨਿਸ਼ਾਨ ਅਤੇ ਡਾਟਾ ਹੁੰਦੇ ਹਨ ਜੋ ਇੱਕ ਵਿਅਕਤੀ ਇੰਟਰਨੈਟ ਵਰਤਦੇ ਸਮੇਂ ਆਪਣੇ ਪਿੱਛੇ ਛੱਡਦਾ ਹੈ, ਅਤੇ ਇਹ ਇੰਟਰਨੈਟ ਦੀ ਦੁਨੀਆ ਵਿੱਚ ਉਸ ਦੀ ਡਿਜਿਟਲ ਪਹਿਚਾਣ ਬਣਾਉਂਦੇ ਹਨ। ਜਦੋਂ ਵੀ ਕੋਈ ਯੂਜ਼ਰ ਵੈਬਸਾਈਟਾਂ 'ਤੇ ਜਾਂਦਾ ਹੈ, ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕੁਝ ਪੋਸਟ ਜਾਂ ਲਾਈਕ ਕਰਦਾ ਹੈ, ਯੂਟਿਊਬ 'ਤੇ ਵੀਡੀਓ ਵੇਖਦਾ ਹੈ, ਗੂਗਲ 'ਤੇ ਖੋਜ ਕਰਦਾ ਹੈ, ਮੇਬਾਈਲ ਐਪਸ ਵਰਤਦਾ ਹੈ, ਆਨਲਾਈਨ ਖਰੀਦਦਾਰੀ ਕਰਦਾ ਹੈ ਜਾਂ ਕਿਸੇ ਵੀ ਤਰ੍ਹਾਂ ਦੀ ਡਿਜਿਟਲ ਸੇਵਾ ਦੀ ਵਰਤੋਂ ਕਰਦਾ ਹੈ, ਤਾਂ ਉਹ ਹਰ ਕਾਰਜ ਇੱਕ ਡਿਜਿਟਲ ਰਿਕਾਰਡ ਬਣਾਉਂਦਾ ਹੈ ਜੋ ਉਸ ਦਾ ਫੁਟਪ੍ਰਿੰਟ ਕਹਾਉਂਦਾ ਹੈ।



ਇਹ ਦੋ ਕਿਸਮਾਂ ਦਾ ਹੁੰਦਾ ਹੈ-ਐਕਟਿਵ ਅਤੇ ਪੈਸਿਵ। ਐਕਟਿਵ ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਉਹ ਹੁੰਦਾ ਹੈ ਜੋ ਯੂਜ਼ਰ ਖੁਦ ਜਾਣ-ਬੁੱਝ ਕੇ ਸਾਂਝਾ ਕਰਦਾ ਹੈ, ਜਿਵੇਂ ਕਿ ਫੇਸਬੁੱਕ ਪੋਸਟ, ਇੰਸਟਾਗ੍ਰਾਮ ਫੋਟੋ, ਯੂਟਿਊਬ ਕਮੈਂਟ, ਬਲੋਗ ਲਿਖਣਾ, ਕੋਈ ਆਨਲਾਈਨ ਫਾਰਮ ਭਰਨਾ ਜਾਂ ਆਪਣੀ ਵਿਅਕਤੀਗਤ ਜਾਣਕਾਰੀ ਦੇਣਾ। ਪੈਸਿਵ ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਉਹ ਹੁੰਦਾ ਹੈ ਜੋ ਆਪਣੇ ਆਪ ਇਕੱਠਾ ਹੁੰਦਾ ਹੈ, ਅਕਸਰ ਬਿਨਾਂ ਯੂਜ਼ਰ ਦੀ ਸਿੱਧੀ ਜਾਣਕਾਰੀ ਦੇ, ਜਿਵੇਂ ਕਿ ਵੈਬਸਾਈਟਾਂ ਦੁਆਰਾ ਕੁਕੀਜ਼ ਰਾਹੀਂ ਇਕੱਠਾ ਕੀਤਾ ਜਾਣ ਵਾਲਾ ਡਾਟਾ, ਸਥਾਨ (ਲੋਕੇਸ਼ਨ) ਟ੍ਰੈਕਿੰਗ, ਬ੍ਰਾਊਜ਼ਿੰਗ ਹਿਸਟਰੀ, ਡਿਵਾਈਸ ਇਨਫਰਮੇਸ਼ਨ, ਐਡ ਟ੍ਰੈਕਿੰਗ ਜਾਂ ਐਪਸ ਦੁਆਰਾ ਬੈਕਗ੍ਰਾਊਂਡ ਵਿੱਚ ਇਕੱਠਾ ਕੀਤਾ ਜਾਣ ਵਾਲਾ ਡਾਟਾ। ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਦਾ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਪਹਿਲੂ ਇਹ ਹੈ ਕਿ ਇੱਕ ਵਾਰ ਕੋਈ ਜਾਣਕਾਰੀ ਇੰਟਰਨੈਟ 'ਤੇ ਆ ਜਾਵੇ, ਤਾਂ ਉਹ ਪੂਰੀ ਤਰ੍ਹਾਂ ਹਟਾਉਣਾ

ਮੁਸ਼ਕਲ ਹੁੰਦਾ ਹੈ, ਇਸ ਲਈ ਇਸਨੂੰ ਡਿਜਿਟਲ ਛਾਪ ਵੀ ਕਿਹਾ ਜਾਂਦਾ ਹੈ। ਇਸ ਛਾਪ ਦਾ ਸਹੀ ਜਾਂ ਗਲਤ ਪ੍ਰਭਾਵ ਭਵਿੱਖ ਵਿੱਚ ਇੱਕ ਵਿਅਕਤੀ ਦੀ ਸਾਖ, ਸੁਰੱਖਿਆ, ਨੌਕਰੀ ਦੇ ਮੌਕੇ ਅਤੇ ਪ੍ਰਾਈਵੇਸੀ 'ਤੇ ਪੈ ਸਕਦਾ ਹੈ। ਕਈ ਕੰਪਨੀਆਂ ਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮ ਇਸ ਫੁਟਪ੍ਰਿੰਟ ਦਾ ਇਸਤੇਮਾਲ ਯੂਜ਼ਰ ਦੇ ਰੁਝਾਨ, ਪਸੰਦ, ਖਰੀਦਦਾਰੀ ਦੇ ਤਰੀਕੇ ਅਤੇ ਆਨਲਾਈਨ ਵਿਹਾਰ ਨੂੰ ਸਮਝਣ ਲਈ ਕਰਦੇ ਹਨ, ਜਿਸ ਦੇ ਆਧਾਰ 'ਤੇ ਉਹ ਵਿਅਕਤੀ ਨੂੰ ਟਾਰਗੇਟ ਕੀਤੀਆਂ ਵਿਗਿਆਪਨ ਦਿਖਾਉਂਦੇ ਹਨ ਜਾਂ ਉਸ ਦੀ ਪ੍ਰੋਫਾਈਲਿੰਗ ਕਰਦੇ ਹਨ। ਜੇਕਰ ਇਹ ਫੁਟਪ੍ਰਿੰਟ ਸੁਰੱਖਿਅਤ ਤਰੀਕੇ ਨਾਲ ਮੈਨੇਜ ਨਾ ਕੀਤਾ ਜਾਵੇ, ਤਾਂ ਹੈਕਰ, ਫਿਸ਼ਿੰਗ ਕਰਨ ਵਾਲੇ ਜਾਂ ਸਾਈਬਰ ਕ੍ਰਿਮਿਨਲ ਇਸ ਜਾਣਕਾਰੀ ਦਾ ਦੁਰੁਪਯੋਗ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਕਰਕੇ ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਦੀ ਸਹੀ ਸਮਝ ਅਤੇ ਇਸਦੀ ਸੰਭਾਲ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇੱਕ ਸੁਰੱਖਿਅਤ ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਬਣਾਉਣ ਲਈ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਵਰਤਣਾ, ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਨੂੰ ਕੱਸ ਕੇ ਰੱਖਣਾ, ਅਣਜਾਣ ਲਿੰਕਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹਿਣਾ, ਬਿਨਾਂ ਲੋੜ ਵਾਲੀਆਂ ਐਪਸ ਨੂੰ ਪਰਮੀਸ਼ਨ ਨਾ ਦੇਣਾ ਅਤੇ ਆਪਣੇ ਆਨਲਾਈਨ ਵਿਹਾਰ ਦੇ ਪ੍ਰਭਾਵ ਨੂੰ ਸਮਝਦੇ ਹੋਏ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ, ਜਿੱਥੇ ਹਰ ਕੰਮ ਆਨਲਾਈਨ ਹੋ ਰਿਹਾ ਹੈ, ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਨੂੰ ਸਮਝਣਾ ਅਤੇ ਇਸਨੂੰ ਕੰਟਰੋਲ ਵਿੱਚ ਰੱਖਣਾ ਇੱਕ ਜ਼ਰੂਰੀ ਡਿਜਿਟਲ ਸਾਖਰਤਾ (digital literacy) ਬਣ ਚੁੱਕੀ ਹੈ, ਕਿਉਂਕਿ ਇਹ ਨਾ ਸਿਰਫ਼ ਤੁਹਾਡੀ ਪ੍ਰਾਈਵੇਸੀ ਦੀ ਰੱਖਿਆ ਕਰਦੀ ਹੈ, ਸਗੋਂ ਤੁਹਾਡੇ ਭਵਿੱਖ ਨੂੰ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਆਨਲਾਈਨ ਨਾਗਰਿਕ ਬਣਨ ਵਿੱਚ ਵੀ ਮਦਦ ਕਰਦੀ ਹੈ।

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਲੋੜ

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਲੋੜ ਇਸ ਕਰਕੇ ਹੈ ਕਿਉਂਕਿ ਆਧੁਨਿਕ ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ ਹਰ ਵਿਅਕਤੀ, ਸੰਸਥਾ ਅਤੇ ਸਰਕਾਰ ਆਪਣੀ ਰੋਜ਼ਾਨਾ ਦੇ ਕੰਮਾਂ ਦਾ ਬਹੁਤ ਸਾਰਾ ਹਿੱਸਾ ਇੰਟਰਨੈੱਟ ਅਤੇ ਡਿਜਿਟਲ ਡਿਵਾਈਸਾਂ ਦੇ ਸਹਾਰੇ ਚਲਾਉਂਦੇ ਹਨ, ਅਤੇ ਇਸ ਡਿਜਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਹਰ ਪਲ ਸਾਈਬਰ ਹਮਲਿਆਂ, ਡਾਟਾ ਚੋਰੀ, ਠੱਗੀ ਅਤੇ ਪ੍ਰਾਈਵੇਸੀ ਉਲੰਘਣ ਦੇ ਖਤਰੇ ਮੌਜੂਦ ਰਹਿੰਦੇ ਹਨ। ਜਿਵੇਂ-ਜਿਵੇਂ ਤਕਨੀਕ ਅੱਗੇ ਵਧ ਰਹੀ ਹੈ, ਹੈਕਰਾਂ ਅਤੇ ਸਾਈਬਰ ਕ੍ਰਿਮਿਨਲਾਂ ਦੇ ਤਰੀਕੇ ਵੀ ਹੋਰ ਅਧੁਨਿਕ ਤੇ ਖਤਰਨਾਕ ਹੋ ਰਹੇ ਹਨ, ਜਿਸ ਨਾਲ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਬੈਂਕਿੰਗ ਡਾਟਾ, ਪਾਸਵਰਡ, ਆਧਾਰ ਜਾਂ ਪਛਾਣ-ਸਬੰਧੀ ਵੇਰਵਾ ਕਈ ਵਾਰ ਬਿਨਾਂ ਜਾਣਕਾਰੀ ਦੇ ਲੀਕ ਹੋ ਜਾਂਦੇ ਹਨ, ਅਤੇ ਇਹ ਡਾਟਾ ਗਲਤ ਹੱਥਾਂ ਵਿੱਚ

ਪੈ ਕੇ ਆਰਥਿਕ ਨੁਕਸਾਨ, ਪ੍ਰਤਿਸ਼ਠਾ ਨੂੰ ਹਾਨੀ ਜਾਂ ਨਕਲੀ ਪਛਾਣ ਬਣਾਉਣ ਵਰਗੇ ਗੰਭੀਰ ਨਤੀਜੇ ਪੈਦਾ ਕਰ ਸਕਦਾ ਹੈ। ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਇਸ ਲਈ ਵੀ ਜ਼ਰੂਰੀ ਹੈ ਕਿਉਂਕਿ ਅੱਜਕੱਲ੍ਹ ਬਹੁਤ ਸਾਰੇ ਸਾਈਬਰ ਹਮਲੇ ਜਿਵੇਂ ਕਿ ਮਾਲਵੇਅਰ, ਰੈਸਮਵੇਅਰ, ਫਿਸ਼ਿੰਗ, ਸੋਸ਼ਲ ਇੰਜੀਨੀਅਰਿੰਗ, ਸਪਾਈਵੇਅਰ ਅਤੇ ਡੀਡੀਓਐਸ ਹਮਲੇ ਖਾਸ ਤੌਰ 'ਤੇ ਯੂਜ਼ਰਾਂ ਨੂੰ ਠੱਗਣ ਜਾਂ ਉਨ੍ਹਾਂ ਦੇ ਡਿਵਾਈਸ ਲੋਕ ਕਰਕੇ ਪੈਸੇ ਵਸੂਲਣ ਲਈ ਕੀਤੇ ਜਾਂਦੇ ਹਨ, ਅਤੇ ਇਹ ਹਮਲੇ ਕਿਸੇ ਵੀ ਸਮੇਂ ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਲਿੰਕ, ਈਮੇਲ ਜਾਂ ਐਪ ਰਾਹੀਂ ਹੋ ਸਕਦੇ ਹਨ। ਕਾਰੋਬਾਰ ਅਤੇ ਸਰਕਾਰੀ ਸੰਸਥਾਵਾਂ ਲਈ ਤਾਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਹੋਰ ਵੀ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿਉਂਕਿ ਉਨ੍ਹਾਂ ਕੋਲ ਲੱਖਾਂ ਲੋਕਾਂ ਦਾ ਸੰਵੇਦਨਸ਼ੀਲ ਡਾਟਾ ਹੁੰਦਾ ਹੈ, ਅਤੇ ਇੱਕ ਛੋਟੀ ਜਿਹੀ ਸਾਈਬਰ ਕਮਜ਼ੋਰੀ ਵੀ ਵੱਡੇ ਆਰਥਿਕ ਨੁਕਸਾਨ, ਡਾਟਾ ਬ੍ਰੀਚ, ਸਰਵਿਸ ਬੰਦ ਹੋਣਾ ਜਾਂ ਰਾਸ਼ਟਰੀ ਸੁਰੱਖਿਆ ਲਈ ਖ਼ਤਰਾ ਪੈਦਾ ਕਰ ਸਕਦੀ ਹੈ। ਇੰਟਰਨੈਟ 'ਤੇ ਵਧ ਰਹੇ ਡਿਜਿਟਲ ਫੁਟਪ੍ਰਿੰਟ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਮੌਜੂਦਗੀ ਕਾਰਨ ਵੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਲੋੜ ਵੱਧ ਗਈ ਹੈ, ਕਿਉਂਕਿ ਕਈ ਯੂਜ਼ਰ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਬਿਲਕੁਲ ਬੇਝਿਜਕ ਸਾਂਝੀ ਕਰਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਹੈਕਰਾਂ ਨੂੰ ਬਿਨਾਂ ਮਿਹਨਤ ਦੇ ਜਾਣਕਾਰੀ ਮਿਲ ਜਾਂਦੀ ਹੈ ਅਤੇ ਉਹ ਇਸਦੀ ਸਹਾਇਤਾ ਨਾਲ ਵਿਅਕਤੀ ਦੀ ਪਛਾਣ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਜਿਵੇਂ-ਜਿਵੇਂ ਆਨਲਾਈਨ ਲੈਣ-ਦੇਣ ਵੱਧ ਰਹੇ ਹਨ, ਨਕਲੀ ਵੈਬਸਾਈਟਾਂ, ਫੇਕ ਕਸਟਮਰ ਕੇਅਰ ਨੰਬਰ, ਯੂਪੀਐਈ ਧੋਖਾਧੜੀ ਅਤੇ ਆਨਲਾਈਨ ਫਿਨਾਂਸ ਠੱਗੀਆਂ ਵੀ ਤੇਜ਼ੀ ਨਾਲ ਵਧ ਰਹੀਆਂ ਹਨ, ਜਿਨ੍ਹਾਂ ਤੋਂ ਬਚਣ ਲਈ ਮਜ਼ਬੂਤ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਆਦਤਾਂ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹਨ। ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਸਿਰਫ਼ ਸੁਰੱਖਿਆ ਸਾਫਟਵੇਅਰ ਜਾਂ ਐਂਟੀਵਾਇਰਸ ਤੱਕ ਸੀਮਤ ਨਹੀਂ ਹੈ; ਇਹ ਵਿਅਕਤੀ ਦੇ ਸਹੀ ਆਨਲਾਈਨ ਵਿਹਾਰ, ਜਾਗਰੂਕਤਾ, ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ, ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA), ਡਾਟਾ ਇਨਕ੍ਰਿਪਸ਼ਨ ਅਤੇ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੇ ਸਹੀ ਇਸਤੇਮਾਲ 'ਤੇ ਵੀ ਨਿਰਭਰ ਕਰਦੀ ਹੈ। ਘਰ, ਸਕੂਲ, ਦਫ਼ਤਰ ਜਾਂ ਕਾਰੋਬਾਰ-ਹਰ ਥਾਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀ ਲੋੜ ਇਸ ਲਈ ਪੈਂਦੀ ਹੈ ਕਿ ਅਸੀਂ ਆਪਣੀ ਡਿਜਿਟਲ ਜ਼ਿੰਦਗੀ ਨੂੰ ਨੁਕਸਾਨ, ਚੋਰੀ ਅਤੇ ਹੋਰਾਫੇਰੀ ਤੋਂ ਬਚਾ ਸਕੀਏ ਅਤੇ ਇੰਟਰਨੈਟ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਵਿਸ਼ਵਾਸਯੋਗ ਅਤੇ ਭਰੋਸੇਮੰਦ ਤਰੀਕੇ ਨਾਲ ਵਰਤ ਸਕੀਏ। ਅੰਤ ਵਿੱਚ, ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਸਿਰਫ਼ ਤਕਨੀਕੀ ਲੋੜ ਨਹੀਂ, ਬਲਕਿ ਆਧੁਨਿਕ ਦੁਨੀਆ ਦੀ ਇੱਕ ਬੁਨਿਆਦੀ ਜ਼ਰੂਰਤ ਹੈ, ਜੋ ਨਿੱਜੀ ਅਤੇ ਸਮੂਹਿਕ ਸੁਰੱਖਿਆ ਲਈ ਅਤਿ ਮਹੱਤਵਪੂਰਨ ਹੈ।

2. ਮਜ਼ਬੂਤ ਅਤੇ ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਬਾਰੇ ਜਾਣਕਾਰੀ

ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣ ਲਈ ਸਭ ਤੋਂ ਜ਼ਰੂਰੀ ਗੱਲ ਇਹ ਹੈ ਕਿ ਉਹ ਮਜ਼ਬੂਤ, ਅਨੁਮਾਨ ਲਾਉਣ ਲਈ ਮੁਸ਼ਕਲ, ਲੰਬਾ ਅਤੇ ਵਿਲੱਖਣ ਹੋਵੇ, ਕਿਉਂਕਿ ਕਮਜ਼ੋਰ ਪਾਸਵਰਡ ਕਿਸੇ ਵੀ ਸਾਈਬਰ ਹਮਲੇ, ਬਰੂਟ-ਫੋਰਸ ਅਟੈਕ ਜਾਂ ਹੈਕਿੰਗ ਤਰੀਕੇ ਨਾਲ ਆਸਾਨੀ ਨਾਲ ਤੋੜੇ ਜਾ ਸਕਦੇ ਹਨ। ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣ ਦੀ ਪਹਿਲੀ ਸ਼ਰਤ ਹੈ ਕਿ ਇਸ ਦੀ ਲੰਬਾਈ ਘੱਟੋ-ਘੱਟ 12 ਤੋਂ 16 ਅੱਖਰ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ, ਕਿਉਂਕਿ ਲੰਮੇ ਪਾਸਵਰਡ ਨੂੰ ਤੋੜਣ ਲਈ ਕਾਫ਼ੀ ਜ਼ਿਆਦਾ ਸਮਾਂ ਅਤੇ ਤਕਨੀਕੀ ਸਾਧਨ ਲੱਗਦੇ ਹਨ। ਦੂਜੀ ਮਹੱਤਵਪੂਰਨ ਗੱਲ ਹੈ ਕਿ ਪਾਸਵਰਡ ਵਿੱਚ ਵੱਡੇ (A-Z) ਅਤੇ ਛੋਟੇ (a-z) ਅੱਖਰਾਂ ਦਾ ਮਿਲਾਪ, ਅੰਕ (0-9) ਅਤੇ ਖਾਸ ਨਿਸ਼ਾਨ ਜਿਵੇਂ ਕਿ @, #, \$, %, &, ! ਆਦਿ ਦਾ ਇਸਤੇਮਾਲ ਕੀਤਾ ਜਾਵੇ, ਤਾਂ ਕਿ ਇਹ ਹੋਰ ਜਟਿਲ ਬਣੇ। ਸਧਾਰਣ ਸ਼ਬਦ, ਆਪਣੇ ਨਾਮ, ਜਨਮ-ਤਾਰੀਖ, ਮੋਬਾਈਲ ਨੰਬਰ ਜਾਂ ਆਸਾਨ ਪੈਟਰਨ ਜਿਵੇਂ 12345, 0000, qwerty, password ਆਦਿ ਕਦੇ ਵੀ ਵਰਤਣੇ ਨਹੀਂ ਚਾਹੀਦੇ, ਕਿਉਂਕਿ ਇਹ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਹੈਕਰਾਂ ਦੀ ਲਿਸਟ ਵਿੱਚ ਹੁੰਦੇ ਹਨ। ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣ ਦਾ ਇੱਕ ਵਧੀਆ ਤਰੀਕਾ ਹੈ passphrase, ਜਿਸ ਵਿੱਚ ਕੁਝ ਬੇਤਰਤੀਬ ਸ਼ਬਦਾਂ ਨੂੰ ਖਾਸ ਚਿੰਨ੍ਹਾਂ ਅਤੇ ਅੰਕਾਂ ਨਾਲ ਮਿਲਾ ਕੇ ਇੱਕ ਲੰਬਾ ਪਰ ਯਾਦ ਰਹਿਣ ਵਾਲਾ ਪਾਸਵਰਡ ਬਣਾਇਆ ਜਾਂਦਾ ਹੈ, ਜਿਵੇਂ ਕਿ “Blue!River92*Moon\$Tree” ਜੋ ਦਿਖਣ ਵਿੱਚ ਜਟਿਲ ਹੈ ਪਰ ਮਨ ਵਿੱਚ ਇੱਕ ਤਸਵੀਰ ਬਣਾਉਣ ਕਰਕੇ ਯਾਦ ਰਹਿ ਸਕਦਾ ਹੈ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਹਰ ਅਕਾਊਂਟ ਲਈ ਵੱਖਰਾ ਪਾਸਵਰਡ ਬਣਾਉਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਕਿਉਂਕਿ ਜੇਕਰ ਇੱਕ ਅਕਾਊਂਟ ਹੈਕ ਹੋ ਜਾਏ ਤਾਂ ਹੋਰ ਸਾਰੇ ਖਾਤੇ ਵੀ ਖਤਰੇ ਵਿੱਚ ਆ ਸਕਦੇ ਹਨ। ਇੱਕ ਹੋਰ ਮਹੱਤਵਪੂਰਨ ਸਿਧਾਂਤ ਹੈ ਪਾਸਵਰਡ ਨੂੰ ਸਮੇਂ-ਸਮੇਂ ‘ਤੇ ਬਦਲਣਾ, ਖਾਸ ਤੌਰ ‘ਤੇ ਜਦੋਂ ਕੋਈ ਸ਼ੱਕ ਵਾਲੀ ਗਤਿਵਿਧੀ ਵੇਖੀ ਜਾਏ ਜਾਂ ਤੁਸੀਂ ਕਿਸੇ ਨਵੀਂ ਡਿਵਾਈਸ, ਪਬਲਿਕ ਵਾਈ-ਫਾਈ ਜਾਂ ਅਜਿਹੇ ਲਿੰਕਾਂ ਦੀ ਵਰਤੋਂ ਕੀਤੀ ਹੋਵੇ ਜੋ ਸੁਰੱਖਿਅਤ ਨਾ ਹੋਣ। ਜੇ ਬਹੁਤ ਸਾਰੇ ਪਾਸਵਰਡ ਯਾਦ ਰੱਖਣਾ ਮੁਸ਼ਕਿਲ ਲੱਗੇ ਤਾਂ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਵਰਤਣਾ ਇੱਕ ਸਭ ਤੋਂ ਸੁਰੱਖਿਅਤ ਵਿਕਲਪ ਹੈ, ਕਿਉਂਕਿ ਇਹ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਂਦਾ, ਸਟੋਰ ਕਰਦਾ ਅਤੇ ਆਟੋ-ਫਿੱਲ ਕਰਦਾ ਹੈ, ਜਿਸ ਨਾਲ ਤੁਸੀਂ ਇੱਕ ਹੀ ਮਜ਼ਬੂਤ ਮਾਸਟਰ ਪਾਸਵਰਡ ਯਾਦ ਰੱਖਣਾ ਹੁੰਦਾ ਹੈ। ਪਾਸਵਰਡ ਨੂੰ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਹੀਂ ਕਰਨਾ ਚਾਹੀਦਾ, ਅਤੇ ਨਾ ਹੀ ਇਸਨੂੰ ਕਿਸੇ ਕਾਗਜ਼ ‘ਤੇ ਸਾਫ਼-ਸਾਫ਼ ਲਿਖ ਕੇ ਐਸੀ ਜਗ੍ਹਾ ਰੱਖਣਾ ਚਾਹੀਦਾ ਹੈ ਜਿੱਥੇ ਹੋਰ ਲੋਕਾਂ ਦੀ ਪਹੁੰਚ ਹੋਵੇ।

ਇਸ ਦੇ ਨਾਲ-ਨਾਲ, ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA) ਹਮੇਸ਼ਾਂ ਚਾਲੂ ਰੱਖਣਾ ਚਾਹੀਦਾ ਹੈ, ਕਿਉਂਕਿ ਜੇ ਪਾਸਵਰਡ ਕੋਈ ਤੋੜ ਵੀ ਲਵੇ, ਤਾਂ ਵੀ 2FA ਇੱਕ ਵਾਧੂ ਸੁਰੱਖਿਆ ਦੀ ਕੰਧ ਬਣਦਾ ਹੈ। ਪਾਸਵਰਡ ਬਣਾਉਂਦੇ ਸਮੇਂ ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਸੀਂ

ਉਹੀ ਚੀਜ਼ ਨਾ ਲਿਖੋ ਜੋ ਕਿਸੇ ਨੂੰ ਤੁਹਾਡੇ ਬਾਰੇ ਜਾਣਕਾਰੀ ਦੇ ਆਧਾਰ 'ਤੇ ਆਸਾਨੀ ਨਾਲ ਮਿਲ ਜਾਵੇ, ਜਿਵੇਂ ਮਨਪਸੰਦ ਟੀਮ, ਪਾਲਤੂ ਜਾਨਵਰ ਦਾ ਨਾਮ ਜਾਂ ਘਰ ਦਾ ਨੰਬਰ। ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੇ ਹਿਸਾਬ ਨਾਲ, ਪਾਸਵਰਡ ਦੀ ਗੁਪਤਤਾ ਅਤੇ ਇਸਦੀ ਜਟਿਲਤਾ ਤੁਹਾਡੇ ਡਿਜ਼ਿਟਲ ਜੀਵਨ ਦੀ ਪਹਿਲੀ ਰੱਖਿਆ-ਲਾਈਨ ਹੁੰਦੀ ਹੈ, ਇਸ ਲਈ ਇੱਕ ਮਜ਼ਬੂਤ, ਵਿਲੱਖਣ ਅਤੇ ਲੰਬਾ ਪਾਸਵਰਡ ਬਣਾਉਣਾ ਹਰ ਡਿਜ਼ਿਟਲ ਯੂਜ਼ਰ ਲਈ ਇੱਕ ਬੁਨਿਆਦੀ ਅਤੇ ਬਹੁਤ ਜ਼ਰੂਰੀ ਕਦਮ ਹੈ, ਜੋ ਤੁਹਾਡੀ ਨਿੱਜਤਾ, ਡਾਟਾ ਅਤੇ ਆਨਲਾਈਨ ਅਕਾਊਂਟਾਂ ਨੂੰ ਸਾਈਬਰ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਵਿੱਚ ਮਦਦ ਕਰਦਾ ਹੈ।

ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਕਿਵੇਂ ਬਣਾਇਆ ਜਾਏ

ਅੱਜ ਦੀ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਉਣਾ ਬਹੁਤ ਹੀ ਜ਼ਰੂਰੀ ਹੈ ਕਿਉਂਕਿ ਕਮਜ਼ੋਰ ਪਾਸਵਰਡ ਹੈਕਰਾਂ ਲਈ ਸਭ ਤੋਂ ਆਸਾਨ ਨਿਸ਼ਾਨਾ ਹੁੰਦੇ ਹਨ। ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਬੈਂਕ ਡਾਟਾ ਅਤੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਬੁਨਿਆਦੀ ਕਵਚ ਹੈ।



1. ਪਾਸਵਰਡ ਕਿੰਨਾ ਲੰਬਾ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ?

ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਦੀ ਲੰਬਾਈ ਘੱਟੋ-ਘੱਟ 12-16 ਅੱਖਰ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ। ਜਿੰਨਾ ਲੰਬਾ ਪਾਸਵਰਡ, ਉਨਾ ਹੀ ਤੇੜਨਾ ਮੁਸ਼ਕਲ।

2. ਵੱਖ-ਵੱਖ ਕਿਸਮ ਦੇ ਅੱਖਰ ਵਰਤੋ

ਪਾਸਵਰਡ ਵਿੱਚ ਹੇਠ ਲਿਖੀਆਂ ਚੀਜ਼ਾਂ ਜ਼ਰੂਰ ਸ਼ਾਮਲ ਕਰੋ:

- ਵੱਡੇ ਅੱਖਰ (A-Z)
- ਛੋਟੇ ਅੱਖਰ (a-z)
- ਅੰਕ (0-9)
- ਖਾਸ ਚਿੰਨ੍ਹ (@, #, \$, %, &, !, ?)

ਇਨ੍ਹਾਂ ਦਾ ਮਿਲਾਪ ਹਮਲਾਵਰਾਂ ਲਈ ਪਾਸਵਰਡ ਦਾ ਅੰਦਾਜ਼ਾ ਲਗਾਉਣਾ ਬਹੁਤ ਮੁਸ਼ਕਲ ਬਣਾ ਦਿੰਦਾ ਹੈ।

3. ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਤੋਂ ਬਚੋ

ਆਪਣਾ ਨਾਮ, ਜਨਮ ਤਾਰੀਖ, ਮੋਬਾਈਲ ਨੰਬਰ ਜਾਂ “123456”, “password” ਜਿਹੇ ਆਸਾਨ ਪਾਸਵਰਡ ਕਦੇ ਨਾ ਵਰਤੋ। ਇਹ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਅਟੈਕਰ ਟਰਾਈ ਕਰਦੇ ਹਨ।

4. ਪਾਸਵਰਡ ਤਕਨੀਕ ਵਰਤੋ

ਪਾਸਵਰਡ ਇੱਕ ਲੰਬਾ ਪਰ ਯਾਦ ਰੱਖਣ ਯੋਗ ਵਾਕ ਹੁੰਦਾ ਹੈ। ਉਦਾਹਰਨ ਲਈ:

“RaaviDaAsta2024!”

ਇਹ ਸੁਰੱਖਿਅਤ ਵੀ ਹੈ ਅਤੇ ਯਾਦ ਵੀ ਰਹਿੰਦਾ ਹੈ।

5. ਹਰ ਥਾਂ ਲਈ ਵੱਖਰਾ ਪਾਸਵਰਡ

ਸਾਰੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਲਈ ਇੱਕੋ ਜਿਹਾ ਪਾਸਵਰਡ ਕਦੇ ਨਾ ਵਰਤੋ। ਜੇਕਰ ਇੱਕ ਖਾਤਾ ਹੈਕ ਹੋ ਜਾਵੇ ਤਾਂ ਸਾਰੇ ਖਾਤੇ ਖਤਰੇ ਵਿੱਚ ਆ ਸਕਦੇ ਹਨ।

6. ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰੋ

ਜੇ ਪਾਸਵਰਡ ਯਾਦ ਰੱਖਣਾ ਮੁਸ਼ਕਲ ਹੋਵੇ ਤਾਂ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਵਰਤੋ। ਇਹ ਟੂਲ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਤਿਆਰ ਵੀ ਕਰਦਾ ਹੈ ਅਤੇ ਸੁਰੱਖਿਅਤ ਤਰੀਕੇ ਨਾਲ ਸੰਭਾਲ ਕੇ ਵੀ ਰੱਖਦਾ ਹੈ।

7. ਸਮੇਂ-ਸਮੇਂ ਤੇ ਪਾਸਵਰਡ ਬਦਲੋ

ਅਹਿਮ ਖਾਤਿਆਂ (ਬੈਂਕ, ਈਮੇਲ) ਦੇ ਪਾਸਵਰਡ ਕੁਝ ਮਹੀਨਿਆਂ ਬਾਅਦ ਬਦਲਣੇ ਚਾਹੀਦੇ ਹਨ।

ਪਾਸਵਰਡ ਨੂੰ ਕਿਸੇ ਨਾਲ ਵੀ ਨਾ ਸਾਂਝਾ ਕਰਨ ਦੀ ਆਦਤ

ਪਾਸਵਰਡ ਨੂੰ ਕਿਸੇ ਨਾਲ ਵੀ ਨਾ ਸਾਂਝਾ ਕਰਨ ਦੀ ਆਦਤ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦਾ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਣ ਅਤੇ ਬੁਨਿਆਦੀ ਨਿਯਮ ਹੈ, ਕਿਉਂਕਿ ਜਦੋਂ ਅਸੀਂ ਆਪਣਾ ਪਾਸਵਰਡ ਸਾਂਝਾ ਕਰਦੇ ਹਾਂ ਤਾਂ ਅਸੀਂ ਆਪਣੇ ਡਿਜ਼ੀਟਲ ਜੀਵਨ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਅਤੇ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਨੂੰ ਖ਼ਤਰੇ ਵਿੱਚ ਪਾ ਦਿੰਦੇ ਹਾਂ; ਪਾਸਵਰਡ ਤੁਹਾਡੀ ਆਨਲਾਈਨ ਪਹਿਚਾਣ ਦੀ ਚਾਬੀ ਹੁੰਦਾ ਹੈ, ਅਤੇ ਜਿਵੇਂ ਕੋਈ ਘਰ ਦੀ ਚਾਬੀ ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ ਨੂੰ ਨਹੀਂ ਦਿੰਦਾ, ਠੀਕ ਉਸੇ ਤਰ੍ਹਾਂ ਪਾਸਵਰਡ ਵੀ ਕਿਸੇ ਨੂੰ ਨਹੀਂ ਦੇਣਾ ਚਾਹੀਦਾ, ਚਾਹੇ ਉਹ ਦੋਸਤ, ਪਰਿਵਾਰਕ ਮੈਂਬਰ, ਕਾਲੀਗ ਜਾਂ ਕੋਈ ਵੀ ਨੇੜਲਾ ਕਿਉਂ ਨਾ ਹੋਵੇ; ਕਈ ਵਾਰ ਲੋਕ ਮਾਸੂਮੀਆਂ ਵਿੱਚ ਸੋਚਦੇ ਹਨ ਕਿ ਪਾਸਵਰਡ ਦੱਸਣ ਨਾਲ ਕੋਈ ਖਾਸ ਸਮੱਸਿਆ ਨਹੀਂ ਹੁੰਦੀ, ਪਰ ਅਸਲ ਵਿੱਚ ਇਹ ਸਭ ਤੋਂ ਵੱਡੀਆਂ ਗ਼ਲਤੀਆਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ, ਕਿਉਂਕਿ ਜਦੋਂ ਵੀ ਪਾਸਵਰਡ ਦੂਜੇ ਦੇ ਹੱਥ ਲੱਗਦਾ ਹੈ, ਉਸਦੀ ਬੇਧਿਆਨੀ, ਗ਼ਲਤੀ ਜਾਂ ਜਾਣਬੁੱਝ ਕੇ ਕੀਤੇ ਗਏ ਗ਼ਲਤ ਇਸਤੇਮਾਲ ਨਾਲ ਅਕਾਊਂਟ ਪੂਰੀ ਤਰ੍ਹਾਂ ਖ਼ਤਰੇ ਵਿੱਚ ਆ ਸਕਦਾ ਹੈ; ਇਹ ਨਾ ਸਿਰਫ਼ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ-ਜਿਵੇਂ ਫੋਟੋਆਂ, ਵੀਡੀਓ, ਚੈਟ, ਦਸਤਾਵੇਜ਼-ਨੂੰ ਅਣਜਾਣ ਲੋਕਾਂ ਦੇ ਸਾਹਮਣੇ ਖੋਲ੍ਹ ਸਕਦਾ ਹੈ, ਪਰ ਤੁਹਾਡੇ ਬੈਂਕਿੰਗ ਅਤੇ ਵਿੱਤੀ ਅਕਾਊਂਟ ਤੱਕ ਪਹੁੰਚ ਵੀ ਪ੍ਰਾਪਤ ਕਰ ਸਕਦਾ ਹੈ, ਜਿਸ ਨਾਲ ਪੈਸੇ ਦੀ ਚੋਰੀ, ਧੋਖਾਧੜੀ, ਬੇਨਾਮ ਲੈਣ-ਦੇਣ ਅਤੇ ਹੋਰ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਦਾ ਖ਼ਤਰਾ ਵੱਧ ਜਾਂਦਾ ਹੈ; ਪਾਸਵਰਡ ਸਾਂਝਾ ਕਰਨ ਨਾਲ ਸਭ ਤੋਂ ਵੱਡਾ ਨੁਕਸਾਨ ਇਹ ਹੁੰਦਾ ਹੈ ਕਿ ਅਸੀਂ ਆਪਣੇ ਅਕਾਊਂਟ ਉੱਤੇ ਕੰਟਰੋਲ ਖੋ ਬੈਠਦੇ ਹਾਂ, ਅਤੇ ਜ਼ਰੂਰੀ ਸਮੇਂ 'ਤੇ ਸਾਬਤ ਨਹੀਂ ਕਰ ਸਕਦੇ ਕਿ ਅਕਾਊਂਟ ਸਾਡਾ ਹੀ ਹੈ, ਕਿਉਂਕਿ ਉਸਦੀ ਵਰਤੋਂ ਕਈ ਲੋਕਾਂ ਦੁਆਰਾ ਕੀਤੀ ਜਾ ਰਹੀ ਹੁੰਦੀ ਹੈ; ਇਸ ਤੋਂ ਇਲਾਵਾ, ਦੋਸਤਾਂ ਜਾਂ ਜਾਣ-ਪਛਾਣ ਵਾਲਿਆਂ 'ਤੇ ਵਿਸ਼ਵਾਸ ਕਰਕੇ ਪਾਸਵਰਡ ਸਾਂਝਾ ਕਰਨਾ ਵੀ ਇੱਕ ਗ਼ਲਤ ਆਦਤ ਹੈ, ਕਿਉਂਕਿ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਰਿਸ਼ਤੇ ਅਤੇ

ਹਾਲਾਤ ਕਦੇ ਵੀ ਬਦਲ ਸਕਦੇ ਹਨ, ਅਤੇ ਅਣਬਣ ਜਾਂ ਗਲਤਫਹਿਮੀਆਂ ਦੇ ਸਮੇਂ ਇੱਕ ਛੋਟੀ ਗ਼ਲਤੀ ਵੀ ਵੱਡੀ ਮੁਸੀਬਤ ਦਾ ਕਾਰਣ ਬਣ ਸਕਦੀ ਹੈ; ਇਸ ਤੋਂ ਇਲਾਵਾ, ਕਈ ਵਾਰ ਲੋਕ ਆਪਣੇ ਕੰਮ ਦੀ ਸਹੂਲਤ ਲਈ ਪਾਸਵਰਡ ਦੂਜਿਆਂ ਨੂੰ ਦੇ ਦਿੰਦੇ ਹਨ, ਜੋ ਕਿ ਪੂਰੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਨੀਤੀ ਦੇ ਉਲਟ ਹੈ, ਕਿਉਂਕਿ ਕੰਪਨੀਆਂ ਅਤੇ ਸੰਸਥਾਵਾਂ ਵਿਚ ਪਾਸਵਰਡ ਸਾਂਝਾ ਕਰਨਾ ਸਭ ਤੋਂ ਵੱਡੀ ਸੁਰੱਖਿਆ ਖਾਮੀ ਮੰਨੀ ਜਾਂਦੀ ਹੈ; ਪਾਸਵਰਡ ਨੂੰ ਸਾਂਝਾ ਨਾ ਕਰਨ ਦੀ ਆਦਤ ਸਿਰਫ ਇਸ ਗੱਲ ਨਾਲ ਨਹੀਂ ਜੁੜੀ ਕਿ ਤੁਸੀਂ ਕਿਸੇ 'ਤੇ ਭਰੋਸਾ ਕਰਦੇ ਹੋ ਜਾਂ ਨਹੀਂ, ਬਲਕਿ ਇਹ ਤੁਹਾਡੀ ਸਵੈ-ਸੁਰੱਖਿਆ, ਜ਼ਿੰਮੇਵਾਰੀ ਅਤੇ ਡਿਜਿਟਲ ਪਰਾਈਵੇਸੀ ਨਾਲ ਵੀ ਜੁੜੀ ਹੈ; ਇਸ ਲਈ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਹਰ ਅਕਾਊਂਟ ਲਈ ਵੱਖਰਾ ਅਤੇ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਇਆ ਜਾਵੇ, ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਉਹਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਥਾਂ ਰੱਖਿਆ ਜਾਵੇ, ਦੇ ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA) ਹਮੇਸ਼ਾਂ ਐਕਟਿਵ ਰੱਖੀ ਜਾਵੇ, ਅਤੇ ਕਿਸੇ ਵੀ ਹਾਲਤ ਵਿੱਚ ਪਾਸਵਰਡ ਕਿਸੇ ਨਾਲ ਵੀ ਸਾਂਝਾ ਨਾ ਕੀਤਾ ਜਾਵੇ; ਇਹ ਆਦਤ ਤੁਹਾਨੂੰ ਸਾਈਬਰ ਹਮਲਿਆਂ, ਹੈਕਿੰਗ, ਡਾਟਾ ਚੋਰੀ ਅਤੇ ਬੇਨਾਮ ਠੱਗੀ ਤੋਂ ਬਚਾਉਂਦੀ ਹੈ ਅਤੇ ਤੁਹਾਡੀ ਡਿਜਿਟਲ ਦੁਨੀਆ ਨੂੰ ਲੰਬੇ ਸਮੇਂ ਲਈ ਸੁਰੱਖਿਅਤ ਅਤੇ ਨਿਯੰਤਰਿਤ ਰੱਖਦੀ ਹੈ।

3. ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਸੁਰੱਖਿਅਤ ਵਰਤੋਂ ਸਬੰਧੀ ਸੁਝਾਅ

ਸੋਸ਼ਲ ਮੀਡੀਆ ਸੁਰੱਖਿਆ ਉਹ ਪ੍ਰਕਿਰਿਆ ਹੈ ਜਿਸ ਨਾਲ ਅਸੀਂ ਆਪਣੇ ਆਨਲਾਈਨ ਅਕਾਊਂਟ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਅਤੇ ਡਿਜ਼ਿਟਲ ਪਹਿਚਾਣ ਨੂੰ ਸਾਈਬਰ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾ ਸਕਦੇ ਹਾਂ, ਕਿਉਂਕਿ ਅੱਜ ਸੋਸ਼ਲ ਮੀਡੀਆ ਠੱਗੀ, ਹੈਕਿੰਗ, ਫਿਸ਼ਿੰਗ ਅਤੇ ਡਾਟਾ ਚੋਰੀ ਦਾ ਸਭ ਤੋਂ ਵੱਡਾ ਨਿਸ਼ਾਨਾ ਬਣ ਚੁੱਕਾ ਹੈ; ਸੁਰੱਖਿਆ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਮਜ਼ਬੂਤ ਅਤੇ ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਵਰਤਣਾ, ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA) ਐਕਟਿਵ ਕਰਨਾ ਅਤੇ ਅਕਾਊਂਟ ਦੀ privacy settings ਨੂੰ ਸਖ਼ਤ ਰੱਖਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ; ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਪਤਾ, ਫੋਨ ਨੰਬਰ, ਸਕੂਲ/ਕਾਲਜ, ਜਾਂ ਸਫ਼ਰ ਦੀਆਂ ਲੋਕੇਸ਼ਨ ਪਬਲਿਕ ਨਾ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ, ਕਿਉਂਕਿ ਇਹ ਜਾਣਕਾਰੀ cyber criminals ਲਈ ਮੌਕਾ ਪੈਦਾ ਕਰਦੀ ਹੈ; ਅਣਜਾਣ ਲੋਕਾਂ ਦੀਆਂ friend requests ਸਵੀਕਾਰ ਕਰਨ ਤੋਂ ਬਚੋ ਅਤੇ ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ ਲਿੰਕ, ਮੈਸੇਜ ਜਾਂ offer 'ਤੇ ਕਲਿਕ ਨਾ ਕਰੋ; ਆਪਣੇ ਪੋਸਟਾਂ ਅਤੇ ਸਟੋਰੀਆਂ ਦੀ visibility "Friends" ਜਾਂ "Close Friends" ਤੱਕ ਹੀ ਸੀਮਿਤ ਰੱਖੋ; ਖਾਤੇ ਦੀ activity ਅਤੇ login sessions ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਚੈਕ ਕਰੋ ਅਤੇ ਜੇ ਕੋਈ ਅਣਜਾਣ device ਦਿਖਾਈ ਦੇਵੇ ਤਾਂ ਤੁਰੰਤ ਲੋਗਆਊਟ ਅਤੇ ਪਾਸਵਰਡ ਬਦਲੋ; Public Wi-Fi 'ਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਵਿੱਚ ਲੋਗਇਨ ਕਰਨ ਤੋਂ ਬਚੋ ਅਤੇ ਜ਼ਰੂਰਤ ਪਏ ਤਾਂ VPN ਇਸਤੇਮਾਲ ਕਰੋ; ਇਹ ਸਾਰੇ ਕਦਮ ਬਹੁਤ ਆਸਾਨ ਹਨ ਪਰ ਇਹ ਤੁਹਾਡੀ ਸੋਸ਼ਲ ਮੀਡੀਆ ਜ਼ਿੰਦਗੀ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਨਿਯੰਤਰਿਤ ਅਤੇ ਹੈਕਿੰਗ ਤੋਂ ਬਚਾਈ ਰੱਖਦੇ ਹਨ।



ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੀ ਮਹੱਤਾ

ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੀ ਮਹੱਤਾ ਆਧੁਨਿਕ ਡਿਜ਼ਿਟਲ ਯੁੱਗ ਵਿੱਚ ਬੇਹੱਦ ਵੱਧ ਗਈ ਹੈ, ਕਿਉਂਕਿ ਅੱਜ ਹਰ ਵਿਅਕਤੀ ਸੋਸ਼ਲ ਮੀਡੀਆ, ਆਨਲਾਈਨ ਸੇਵਾਵਾਂ, ਮੋਬਾਈਲ ਐਪਸ ਅਤੇ ਵੈਬਸਾਈਟਾਂ ਰਾਹੀਂ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਬਿਨਾਂ ਜਾਣ-ਬੂਝੇ ਸਾਂਝੀ ਕਰ ਰਿਹਾ ਹੈ; ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਉਹ ਸੁਰੱਖਿਆ ਰੱਖਵਾਲੇ ਹਨ ਜੋ ਇਹ ਨਿਰਧਾਰਤ ਕਰਦੇ ਹਨ ਕਿ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਕੌਣ ਦੇਖ ਸਕਦਾ ਹੈ, ਕਿਵੇਂ ਵਰਤ ਸਕਦਾ ਹੈ ਅਤੇ ਕਿਹੜੇ ਹਾਲਾਤਾਂ ਵਿੱਚ ਉਸ ਤੱਕ ਪਹੁੰਚ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ, ਇਸ ਲਈ ਇਹ ਨਿੱਜਤਾ, ਸੁਰੱਖਿਆ ਅਤੇ ਆਨਲਾਈਨ ਪਹਿਚਾਣ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਬੇਹੱਦ ਜ਼ਰੂਰੀ ਹਨ; ਜੇ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਠੀਕ ਤਰੀਕੇ ਨਾਲ ਕਨਫਿਗਰ ਨਹੀਂ ਕੀਤੀਆਂ ਜਾਂਦੀਆਂ, ਤਾਂ cyber criminals, ਹੇਕਰਸ, stalkers ਜਾਂ ਤੀਜੀਆਂ ਪਾਰਟੀਆਂ ਵੱਲੋਂ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਆਸਾਨੀ ਨਾਲ ਇਸਤੇਮਾਲ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ—ਜਿਵੇਂ ਕਿ ਫੋਟੋਆਂ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਸਥਾਨ (location), contacts ਜਾਂ ਹੋਰ ਸੰਵੇਦਨਸ਼ੀਲ ਡਾਟਾ—ਜੋ ਸਾਈਬਰ ਬੁੱਲਿੰਗ, ਠੱਗੀ, impersonation, identity theft ਅਤੇ blackmail ਵਰਗੀਆਂ ਸਮੱਸਿਆਵਾਂ ਨੂੰ ਜਨਮ ਦੇ ਸਕਦਾ ਹੈ; ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੀ ਮਹੱਤਾ ਇਸ ਗੱਲ ਨਾਲ ਵੀ ਜੁੜੀ ਹੈ ਕਿ ਇਹ ਤੁਹਾਨੂੰ ਆਪਣੀ ਆਨਲਾਈਨ ਪਹਿਚਾਣ ਉੱਤੇ ਪੂਰਾ ਕੰਟਰੋਲ ਦਿੰਦੀ ਹੈ, ਕਿਉਂਕਿ ਤੁਸੀਂ ਫੈਸਲਾ ਕਰਦੇ ਹੋ ਕਿ ਕਿਹੜੀਆਂ ਪੋਸਟਾਂ ਪਬਲਿਕ ਦਿਖਣਗੀਆਂ, ਕਿਹੜੀਆਂ ਸਿਰਫ਼ ਦੋਸਤਾਂ ਲਈ ਅਤੇ ਕਿਹੜੀਆਂ ਸਿਰਫ਼ ਤੁਹਾਡੇ ਲਈ, ਅਤੇ ਇਸ ਨਾਲ ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਸੁਰੱਖਿਅਤ ਵਰਤੋਂ ਸੰਭਵ ਹੁੰਦੀ ਹੈ; ਇਸ ਦੇ ਨਾਲ ਨਾਲ, ਮਜ਼ਬੂਤ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਆਨਲਾਈਨ ਹੈਰਾਸਮੈਂਟ ਤੋਂ ਬਚਾਉਂਦੀਆਂ ਹਨ, ਕਿਉਂਕਿ ਜਦੋਂ ਤੁਹਾਡੀ ਪ੍ਰੋਫਾਈਲ ਪਬਲਿਕ ਨਹੀਂ ਹੁੰਦੀ, ਤਾਂ ਅਣਜਾਣ ਲੋਕ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਨਹੀਂ ਕਰ ਸਕਦੇ, ਜਿਸ ਨਾਲ ਨਕਲੀ ਅਕਾਊਂਟ ਬਣਾਉਣ, ਸ਼ਰਾਰਤੀ ਕਮੈਂਟ ਪਾਉਣ ਜਾਂ ਗਲਤ ਤਰੀਕੇ ਨਾਲ ਸਮੱਗਰੀ ਦੀ ਵਰਤੋਂ ਕਰਨ ਦਾ ਖ਼ਤਰਾ ਘਟ ਜਾਂਦਾ ਹੈ; ਇਸ ਤੋਂ ਇਲਾਵਾ, ਕਈ ਵੈਬਸਾਈਟਾਂ ਅਤੇ ਐਪਸ ਤੁਹਾਡਾ ਡਾਟਾ ਵਿਗਿਆਪਨ ਜਾਂ ਵਿਸ਼ਲੇਸ਼ਣ ਲਈ ਇਕੱਠਾ ਕਰਦੀਆਂ ਹਨ, ਅਤੇ ਜੇ ਤੁਸੀਂ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਨੂੰ ਠੀਕ ਤਰੀਕੇ ਨਾਲ ਨਹੀਂ ਸੈਟ ਕਰਦੇ, ਤਾਂ ਤੁਹਾਡਾ ਡਾਟਾ ਤੀਜੀਆਂ ਕੰਪਨੀਆਂ ਨੂੰ ਵੇਚਿਆ ਜਾਂ ਸਾਂਝਾ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ, ਜਿਸ ਨਾਲ Targeted ਐਡਵਰਟਾਈਜ਼ਮੈਂਟਾਂ, ਪ੍ਰੋਫਾਈਲਿੰਗ ਅਤੇ ਡਾਟਾ ਮਾਈਨਿੰਗ ਹੋ ਸਕਦੀ ਹੈ; ਇਸ ਲਈ privacy settings ਤੁਹਾਨੂੰ ਇਹ ਚੋਣ ਕਰਨ ਦਾ ਹੱਕ ਦਿੰਦੀਆਂ ਹਨ ਕਿ ਕਿਹੜੀ ਜਾਣਕਾਰੀ ਐਪ ਜਾਂ ਪਲੇਟਫਾਰਮ ਸਾਂਝੀ ਕਰ ਸਕਦਾ ਹੈ ਅਤੇ ਕਿਹੜੀ ਨਹੀਂ; ਬੱਚਿਆਂ ਅਤੇ ਨੌਜਵਾਨਾਂ ਲਈ ਤਾਂ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਹੋਰ ਵੀ ਜ਼ਰੂਰੀ ਹਨ, ਕਿਉਂਕਿ ਉਹ ਅਕਸਰ ਬਿਨਾਂ ਸੋਚੇ ਸਮੱਗਰੀ ਪੋਸਟ ਕਰ ਦਿੰਦੇ ਹਨ ਅਤੇ ਆਪਣੀ ਸੁਰੱਖਿਆ ਨੂੰ ਖਤਰੇ ਵਿੱਚ ਪਾ ਦੇਂਦੇ ਹਨ, ਇਸ ਲਈ ਮਾਤਾ-ਪਿਤਾ ਲਈ parental controls ਅਤੇ profile visibility ਦੇ ਵਿਕਲਪ ਬਹੁਤ ਲਾਭਦਾਇਕ ਹਨ।

ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੀ ਮਹੱਤਾ ਕੰਪਨੀ ਲਈ ਵੀ ਬਰਾਬਰ ਹੈ, ਕਿਉਂਕਿ ਕਰਮਚਾਰੀਆਂ ਦੀ ਜਾਣਕਾਰੀ ਲੀਕ ਹੋਣਾ, ਗੁਪਤ ਡਾਟਾ ਬਾਹਰ ਆਉਣਾ ਅਤੇ ਧੰਦਿਆਂ ਵਿੱਚ ਜਾਸੂਸੀ ਹੋਣਾ ਵਪਾਰ ਲਈ ਵੱਡਾ ਨੁਕਸਾਨ ਹੋ ਸਕਦਾ ਹੈ; ਇਸ ਤਰ੍ਹਾਂ, ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਨਾ ਸਿਰਫ਼ ਸਾਈਬਰ ਹਮਲੇ ਅਤੇ ਡਾਟਾ ਚੋਰੀ ਤੋਂ ਸੁਰੱਖਿਆ ਕਰਦੀਆਂ ਹਨ, ਸਗੋਂ ਤੁਹਾਡੀ ਨਿੱਜਤਾ ਦੀ ਰੱਖਿਆ, ਡਿਜਿਟਲ footprint ਨੂੰ ਨਿਯੰਤਰਿਤ ਕਰਨ ਅਤੇ ਆਨਲਾਈਨ ਜੀਵਨ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਣ ਲਈ ਬੁਨਿਆਦੀ ਢਾਲ ਵਜੋਂ ਕੰਮ ਕਰਦੀਆਂ ਹਨ; ਇਸ ਲਈ, ਹਰ ਵਰਤੋਂਕਾਰ ਨੂੰ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਆਪਣੀਆਂ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ, ਉਹਨਾਂ ਨੂੰ ਅਪਡੇਟ ਰੱਖਣਾ ਚਾਹੀਦਾ ਹੈ ਅਤੇ ਹਰ ਪਲੇਟਫਾਰਮ 'ਤੇ ਜ਼ਰੂਰੀ ਸੀਮਾਵਾਂ ਲਗਾਕੇ ਆਪਣੀ ਡਿਜਿਟਲ ਸੁਰੱਖਿਆ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਉਣਾ ਚਾਹੀਦਾ ਹੈ।

ਫੇਕ ਪ੍ਰੋਫਾਈਲਾਂ ਦੀ ਪਛਾਣ

ਫੇਕ ਪ੍ਰੋਫਾਈਲਾਂ ਦੀ ਪਛਾਣ ਆਧੁਨਿਕ ਡਿਜਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਬਹੁਤ ਹੀ ਮਹੱਤਵਪੂਰਨ ਹੁੰਦੀ ਜਾ ਰਹੀ ਹੈ, ਕਿਉਂਕਿ ਵੱਧ ਰਹੀਆਂ ਠੱਗੀਆਂ, ਹੈਕਿੰਗ ਦੇ ਮਾਮਲੇ, ਆਨਲਾਈਨ ਬੁੱਲਿੰਗ ਅਤੇ ਡਾਟਾ ਚੋਰੀ ਦੇ ਖਤਰੇ ਹੁਣ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਨਕਲੀ ਪ੍ਰੋਫਾਈਲਾਂ ਬਣਾਉਣ ਨਾਲ ਸਿੱਧੇ ਜੁੜੇ ਹੋਏ ਹਨ; ਇੱਕ ਫੇਕ ਪ੍ਰੋਫਾਈਲ ਦੀ ਪਛਾਣ ਕਰਨ ਦਾ ਪਹਿਲਾ ਸੰਕੇਤ ਹੁੰਦਾ ਹੈ—ਅਸਲੀ ਫੋਟੋਆਂ ਦੀ ਗੈਰਹਾਜ਼ਰੀ ਜਾਂ ਗੂਗਲ ਤੋਂ ਚੋਰੀ ਕੀਤੀਆਂ ਤਸਵੀਰਾਂ ਦੀ ਵਰਤੋਂ, ਕਿਉਂਕਿ ਨਕਲੀ ਪ੍ਰੋਫਾਈਲ ਅਕਸਰ overly-perfect, ਮਾਡਲ ਜਿਹੀਆਂ ਫੋਟੋਆਂ ਵਰਤਦੇ ਹਨ ਜਾਂ ਇੱਕੋ ਤਸਵੀਰ ਨੂੰ ਕਈ ਥਾਵਾਂ 'ਤੇ ਰਪੀਟ ਕਰਦੇ ਹਨ



ਦੂਜਾ ਸੰਕੇਤ ਹੁੰਦਾ ਹੈ ਬਹੁਤ ਘੱਟ ਜਾਂ ਬਹੁਤ ਜ਼ਿਆਦਾ followers/friends — ਨਕਲੀ ਪ੍ਰੋਫਾਈਲਾਂ ਵਿੱਚ ਅਕਸਰ ਹੁੰਦਾ ਹੈ ਕਿ ਦੇਸਤ ਘੱਟ ਹੁੰਦੇ ਹਨ ਪਰ likes, comments ਜਾਂ followers ਅਸਮਾਨ ਜਾਂ ਅਣਜਾਣ ਲੋਕਾਂ ਦੇ ਹੁੰਦੇ ਹਨ; ਤੀਜਾ ਲੱਛਣ ਹੈ incomplete bio ਜਾਂ ਕੁਝ ਵੀ personal information ਨਾ ਦੇਣਾ, ਕਿਉਂਕਿ ਠੱਗ ਪ੍ਰੋਫਾਈਲ ਅਕਸਰ ਆਪਣੀ ਪਹਿਚਾਣ

ਨੂੰ ਛੁਪਾਉਣ ਲਈ About section ਨੂੰ ਖਾਲੀ ਰੱਖਦੇ ਹਨ; ਚੋਥਾ ਸੰਕੇਤ ਹੈ unusual behavior — ਜਿਵੇਂ ਬਹੁਤ ਜਲਦੀ ਤਸਵੀਰਾਂ 'ਤੇ like/comment ਕਰਨਾ, ਬਿਨਾਂ ਜਾਣ-ਪਛਾਣ inbox ਵਿੱਚ ਮੈਸੇਜ ਕਰਨਾ, emotional trust ਬਣਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨਾ ਜਾਂ ਪੈਸਾ ਮੰਗਣ ਵਾਲੇ ਸੰਦੇਸ਼; ਪੰਜਵਾਂ ਸੰਕੇਤ ਹੈ language pattern — ਨਕਲੀ ਪ੍ਰੋਫਾਈਲ ਅਕਸਰ ਇੱਕੋ ਕਿਸਮ ਦੇ ਜਵਾਬ, copy-paste ਵਾਲੀ language ਜਾਂ robotic style ਦੇ messages ਭੇਜਦੇ ਹਨ, ਕਿਉਂਕਿ ਉਹ automated scripts ਜਾਂ ਫਰਾਡ ਟੀਮ ਦੁਆਰਾ ਚਲਾਉਣੇ ਹੁੰਦੇ ਹਨ; ਛੇਵਾਂ ਲੱਛਣ suspicious links — fake accounts ਅਕਸਰ links ਭੇਜਦੇ ਹਨ ਜੋ ਫਿਸ਼ਿੰਗ ਵੈਬਸਾਈਟਾਂ ਵੱਲ ਲੈ ਜਾਂਦੇ ਹਨ, ਜੋ ਤੁਹਾਡੀ personal information, passwords ਜਾਂ banking details ਚੁਰਾਉਣ ਲਈ ਬਣੇ ਹੋਏ ਹਨ; ਸੱਤਵਾਂ ਸੰਕੇਤ mutual friends ਦੀ ਗੈਰਮੌਜੂਦਗੀ — ਜੇ ਇੱਕ ਅਜਿਹੇ ਪ੍ਰੋਫਾਈਲ ਤੋਂ friend request ਆਉਂਦੀ ਹੈ ਜਿਸਦੇ mutual ਕੋਈ ਨਹੀਂ, ਉਹ ਨਵਾਂ ਹੈ ਅਤੇ ਬਹੁਤ ਘੱਟ activity ਰੱਖਦਾ ਹੈ, ਤਾਂ ਇਹ ਜ਼ਿਆਦਾਤਰ fake ਹੁੰਦਾ ਹੈ; ਅੱਠਵਾਂ ਸੰਕੇਤ account activity — ਫੇਕ ਪ੍ਰੋਫਾਈਲ ਅਕਸਰ ਕੁਝ ਹੀ ਦਿਨ ਪੁਰਾਣੇ ਹੁੰਦੇ ਹਨ, ਪਰ ਉਨ੍ਹਾਂ 'ਤੇ ਅਸਧਾਰਨ ਤੌਰ 'ਤੇ ਬਹੁਤ ਸਾਰੀਆਂ photos, likes ਅਤੇ posts ਹੁੰਦੀਆਂ ਹਨ ਜੋ ਅਸਲ ਜ਼ਿੰਦਗੀ ਦੀ ਲਗਾਤਾਰ activity ਨਾਲ ਮਿਲਦੀਆਂ ਨਹੀਂ; ਨੌਵਾਂ ਸੰਕੇਤ overly friendly behavior — ਇੱਕਦਮ ਤੋਂ personal information ਪੁੱਛਣਾ, video call ਲਈ ਜ਼ੋਰ ਪਾਉਣਾ ਜਾਂ romantic messages ਭੇਜਣਾ romance scams ਦੀ ਸ਼ੁਰੂਆਤ ਹੋ ਸਕਦੀ ਹੈ; ਦਸਵਾਂ ਲੱਛਣ reverse image search — ਜੇ ਤੁਸੀਂ profile ਦੀ image ਨੂੰ Google reverse image search 'ਤੇ ਚੈਕ ਕਰੋ ਅਤੇ ਉਹ ਕਈ ਅਣਜਾਣ ਵੈਬਸਾਈਟਾਂ ਜਾਂ ਮਾਡਲਿੰਗ ਪੋਰਟਲਾਂ ਤੋਂ ਮਿਲਦੀ ਹੈ, ਤਾਂ ਇਹ 100% fake profile ਹੁੰਦੀ ਹੈ; ਫੇਕ ਪ੍ਰੋਫਾਈਲਾਂ ਦੀ ਪਛਾਣ ਲਈ ਹਮੇਸ਼ਾਂ skepticism ਅਤੇ “verify before trust” ਵਾਲੀ ਸੋਚ ਰੱਖੋ, ਪਰਦੇਦਾਰੀ ਸੈਟਿੰਗਾਂ ਨੂੰ ਮਜ਼ਬੂਤ ਰੱਖੋ, friend requests thoughtfully accept ਕਰੋ ਅਤੇ ਕੋਈ ਵੀ personal detail, OTP, password ਜਾਂ banking ਜਾਣਕਾਰੀ ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ ਪ੍ਰੋਫਾਈਲ ਨਾਲ share ਨਾ ਕਰੋ; ਇਨ੍ਹਾਂ ਤਰੀਕਿਆਂ ਨਾਲ ਤੁਸੀਂ ਨਾ ਸਿਰਫ ਫੇਕ ਪ੍ਰੋਫਾਈਲਾਂ ਦੀ ਪਛਾਣ ਕਰ ਸਕਦੇ ਹੋ, ਸਗੋਂ ਆਪਣੀ ਡਿਜਿਟਲ ਸੁਰੱਖਿਆ ਨੂੰ ਵੀ ਮਜ਼ਬੂਤ ਅਤੇ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹੋ।

ਓਵਰਸ਼ੇਅਰਿੰਗ ਤੋਂ ਬਚਾਅ

ਓਵਰਸ਼ੇਅਰਿੰਗ ਤੋਂ ਬਚਾਅ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਲਈ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ, ਕਿਉਂਕਿ ਅੱਜ ਦੇ ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ ਲੋਕ ਬਿਨਾਂ ਸੋਚੇ ਸਮਝੇ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ—ਜਿਵੇਂ ਫੋਟੋਆਂ, ਸਥਾਨ (location), ਦਿਨਚਰਿਆ, ਪਰਿਵਾਰਕ ਵੇਰਵੇ, ਸਕੂਲ/ਕਾਲਜ ਦੀ ਜਾਣਕਾਰੀ, ਕੰਮ ਵਾਲੀ ਜਗ੍ਹਾ ਅਤੇ ਸਫ਼ਰ ਦੇ ਪਲਾਨ—ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਪੋਸਟ ਕਰ ਦਿੰਦੇ ਹਨ, ਜੋ cyber criminals ਲਈ ਵੱਡਾ ਮੌਕਾ ਪੈਦਾ ਕਰਦੀ ਹੈ।



ਓਵਰਸ਼ੇਅਰਿੰਗ ਨਾਲ identity theft, stalking, blackmailing, cyberbullying ਅਤੇ even house burglary ਜਿਹੇ ਖਤਰੇ ਵਧ ਜਾਂਦੇ ਹਨ, ਕਿਉਂਕਿ ਜੇ ਕੋਈ ਜਾਣਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਕਿੱਥੇ ਹੋ ਜਾਂ ਕਦੋਂ ਘਰ ਨਹੀਂ ਹੋਵੋਗੇ, ਤਾਂ ਉਹ ਇਸਦਾ ਗਲਤ ਇਸਤੇਮਾਲ ਕਰ ਸਕਦਾ ਹੈ; ਇਸ ਤੋਂ ਬਚਾਅ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ privacy settings ਨੂੰ ਸਮਝ ਰੱਖੋ ਅਤੇ ਆਪਣੀਆਂ ਪੋਸਟਾਂ ਦੀ visibility ਸਿਰਫ਼ trusted people ਲਈ ਸੀਮਿਤ ਕਰੋ; location sharing ਬੰਦ ਰੱਖੋ ਅਤੇ ਕਿਸੇ ਵੀ event ਜਾਂ trip ਦੀਆਂ photos real-time 'ਚ ਪੋਸਟ ਕਰਨ ਦੀ ਬਜਾਏ ਬਾਅਦ ਵਿੱਚ ਕਰੋ; ਬੱਚਿਆਂ ਦੀਆਂ photos ਪੋਸਟ ਕਰਨ ਸਮੇਂ extra care ਰੱਖੋ, ਕਿਉਂਕਿ ਇੱਕ ਛੋਟੀ ਜਾਣਕਾਰੀ ਵੀ online predators ਲਈ ਖਤਰਾ ਬਣ ਸਕਦੀ ਹੈ; personal documents, IDs, tickets, address, phone number ਵਰਗੀ ਜਾਣਕਾਰੀ ਕਦੇ ਵੀ share ਨਾ ਕਰੋ; followers ਜਾਂ friends ਦੀ ਗਿਣਤੀ ਵਧਾਉਣ ਲਈ ਅਣਜਾਣ ਲੋਕਾਂ ਨੂੰ add ਨਾ ਕਰੋ; ਆਪਣੀਆਂ old posts ਅਤੇ tags ਨੂੰ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ

ਚੈਕ ਕਰਕੇ ਬੇਲੋੜੀ ਜਾਣਕਾਰੀ ਹਟਾਓ; ਸਭ ਤੋਂ ਵੱਡੀ ਗੱਲ-ਹਰ ਵਾਰ “Share” ‘ਤੇ click ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚੋ ਕਿ ਕੀ ਇਹ ਜਾਣਕਾਰੀ ਕਿਸੇ ਗਲਤ ਵਿਅਕਤੀ ਦੇ ਹੱਥ ਲੱਗ ਕੇ ਮੁਸੀਬਤ ਪੈਦਾ ਕਰ ਸਕਦੀ ਹੈ; ਇਹ ਸਧਾਰਣ ਸਾਵਧਾਨੀਆਂ ਤੁਹਾਨੂੰ ਓਵਰਸ਼ੇਅਰਿੰਗ ਦੇ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾਉਂਦੀਆਂ ਹਨ ਅਤੇ ਤੁਹਾਡੀ ਡਿਜਿਟਲ ਨਿੱਜਤਾ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਦੀਆਂ ਹਨ।

ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦੀ ਪਛਾਣ ਤੇ ਰਿਪੋਰਟਿੰਗ

ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦੀ ਪਛਾਣ ਤੇ ਰਿਪੋਰਟਿੰਗ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਅਤੇ ਮਨੋਵਿਗਿਆਨਕ ਭਲਾਈ ਲਈ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ, ਕਿਉਂਕਿ ਡਿਜਿਟਲ ਮਾਧਿਅਮਾਂ ਰਾਹੀਂ ਹੋਣ ਵਾਲੀ ਤੰਗ-ਪਰੇਸ਼ਾਨੀ ਅਕਸਰ ਚੁੱਪਚਾਪ ਹੁੰਦੀ ਹੈ ਅਤੇ ਕਈ ਵਾਰ ਪੀੜਤ ਨੂੰ ਸਮਝ ਨਹੀਂ ਆਉਂਦਾ ਕਿ ਉਹ ਬੁੱਲਿੰਗ ਦਾ ਸ਼ਿਕਾਰ ਹੋ ਰਿਹਾ ਹੈ; ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦੀ ਪਛਾਣ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਇਹ ਦੇਖੋ ਕਿ ਕੋਈ ਵਿਅਕਤੀ ਮੁੜ-ਮੁੜ ਅਪਮਾਨਜਨਕ ਕਮੈਂਟ ਕਰਦਾ ਹੈ, ਧਮਕੀ ਭਰੇ ਮੈਸੇਜ ਭੇਜਦਾ ਹੈ, ਤੁਹਾਡੀ ਇਜ਼ਜ਼ਤ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦਾ ਹੈ ਜਾਂ ਤੁਹਾਡੇ ਬਾਰੇ ਝੂਠੀ ਜਾਣਕਾਰੀ ਫੈਲਾਉਂਦਾ ਹੈ; ਇਸ ਦੇ ਇਲਾਵਾ, ਕੋਈ ਤੁਹਾਡੀਆਂ ਫੋਟੋਆਂ ਨੂੰ ਬਿਨਾਂ ਇਜਾਜ਼ਤ share ਕਰੇ, ਨਕਲੀ ਪ੍ਰੋਫਾਈਲ ਬਣਾਕੇ ਤੁਹਾਡਾ ਮਖੌਲ ਉਡਾਏ, ਹਮੇਸ਼ਾਂ ਨਿਗੋਟਿਵ ਰੀਐਕਸ਼ਨ ਦੇਵੇ ਜਾਂ ਤੁਹਾਨੂੰ ਡਰਾਉਣ ਵਾਲੀਆਂ online activities ਕਰੇ, ਤਾਂ ਇਹ ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦੇ ਸਪਸ਼ਟ ਸੰਕੇਤ ਹਨ; ਜਦੋਂ ਵੀ ਤੁਸੀਂ ਇਹ ਲੱਛਣ ਵੇਖੋ, ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਬੁਲੀਅਰ ਨਾਲ direct ਬਹਿਸ ਨਾ ਕਰੋ-ਨਾਂ ਉਹਨਾਂ ਨੂੰ reply ਕਰੋ, ਨਾਂ ਹੀ ਉਨ੍ਹਾਂ ਦੀਆਂ ਧਮਕੀਆਂ ਦਾ ਡਰ ਦਿਖਾਓ; ਸਾਰੇ messages, screenshots, links ਅਤੇ timestamps ਨੂੰ proof ਵਜੋਂ ਸੰਭਾਲੋ; ਇਸ ਤੋਂ ਬਾਅਦ, ਉਸ ਵਿਅਕਤੀ ਨੂੰ ਤੁਰੰਤ block ਕਰੋ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮ ਦੇ “Report” option ਰਾਹੀਂ ਉਸਦੀ ਹਰਕਤ ਦੀ ਸ਼ਿਕਾਇਤ ਕਰੋ, ਕਿਉਂਕਿ ਹਰ ਵੱਡਾ ਪਲੇਟਫਾਰਮ bullying, harassment ਅਤੇ hate content ਦੇ ਖਿਲਾਫ ਸਖ਼ਤ ਕਾਰਵਾਈ ਕਰਦਾ ਹੈ; ਜੇ ਬੁੱਲਿੰਗ ਗੰਭੀਰ ਹੈ ਜਾਂ personal harm, blackmail ਜਾਂ ਸ਼ਰਮਿੰਦਗੀ ਵਾਲੀ ਸਮੱਗਰੀ ਸਾਂਝੀ ਕਰਨ ਦੀ ਧਮਕੀ ਮਿਲੇ, ਤਾਂ ਇਹ ਮਾਮਲਾ ਮਾਪਿਆਂ, ਅਧਿਆਪਕਾਂ, ਸਕੂਲ ਪ੍ਰਬੰਧਕਾਂ ਜਾਂ ਸਾਈਬਰ ਸੈੱਲ ਨੂੰ ਤੁਰੰਤ ਰਿਪੋਰਟ ਕਰੋ; ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਗੱਲ ਇਹ ਹੈ ਕਿ ਬੁੱਲਿੰਗ ਨੂੰ ਕਦੇ ਵੀ ਅਣਡਿੱਠਾ ਨਾ ਛੱਡੋ-ਆਪਣੀ ਮਾਨਸਿਕ ਸਿਹਤ ਦੀ ਸੰਭਾਲ ਕਰੋ, ਭਰੋਸੇਮੰਦ ਲੋਕਾਂ ਨਾਲ ਗੱਲ ਕਰੋ ਅਤੇ ਯਕੀਨ ਰੱਖੋ ਕਿ ਸਹੀ ਰਿਪੋਰਟਿੰਗ ਨਾਲ cyber bullying ਦਾ ਅੰਤ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ।

4. ਸਾਈਬਰ ਬੁੱਲਿੰਗ (Cyberbullying) ਅਤੇ ਇਸ ਤੋਂ ਬਚਾਵ ਦੇ ਤਰੀਕੇ

ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਉਹ ਦੁਰਵਿਵਹਾਰ ਹੈ ਜੋ ਇੰਟਰਨੈਟ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਮੋਬਾਈਲ ਫੋਨ, ਇਮੇਲ ਜਾਂ ਕਿਸੇ ਵੀ ਡਿਜਿਟਲ ਪਲੇਟਫਾਰਮ ਰਾਹੀਂ ਕਿਸੇ ਵਿਅਕਤੀ ਨੂੰ ਤੰਗ ਕਰਨ, ਡਰਾਉਣ, ਬੇਇਜ਼ਤ ਕਰਨ ਜਾਂ ਮਨੋਵਿਗਿਆਨਕ ਤੌਰ 'ਤੇ ਹਾਨੀ ਪਹੁੰਚਾਉਣ ਲਈ ਕੀਤਾ ਜਾਂਦਾ ਹੈ, ਅਤੇ ਇਹ ਅੱਜ ਦੇ ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ ਸਭ ਤੋਂ ਵੱਧ ਫੈਲਦਾ ਜਾ ਰਿਹਾ ਸਮੱਸਿਆਵਾਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ; ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦੀ ਸ਼ਕਲ ਵੱਖ-ਵੱਖ ਹੋ ਸਕਦੀ ਹੈ, ਜਿਵੇਂ ਕਿ ਕਿਸੇ ਨੂੰ ਅਪਮਾਨਜਨਕ ਜਾਂ ਧਮਕੀ ਭਰੇ ਮੈਸੇਜ ਭੇਜਣਾ, ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਉਸ ਬਾਰੇ ਝੂਠੇ ਦੋਸ਼ ਲਗਾਉਣਾ, ਬਿਨਾਂ ਇਜਾਜ਼ਤ ਫੋਟੋਆਂ ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਪੋਸਟ ਕਰਨਾ, ਕਿਸੇ ਦੀ ਨਕਲੀ ਪ੍ਰੋਫਾਈਲ ਬਣਾਉਣਾ, ਉਸਦਾ ਮਖੌਲ ਉਡਾਉਂਦੇ ਜਾਲਸਾਜ਼ੀ ਭਰੇ ਕਮੈਂਟ ਕਰਨਾ ਜਾਂ ਉਸਨੂੰ ਜਨਤਕ ਤੌਰ 'ਤੇ ਸ਼ਰਮਿੰਦਾ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨਾ।



ਇਹ ਬੁੱਲਿੰਗ ਆਮ ਤੌਰ 'ਤੇ ਛੁਪੇ ਤਰੀਕੇ ਨਾਲ ਹੁੰਦੀ ਹੈ ਕਿਉਂਕਿ ਬੁਲੀਅਰ anonymous ਰਹਿ ਸਕਦਾ ਹੈ, ਜਿਸ ਨਾਲ ਪੀੜਤ ਨੂੰ ਇਹ ਪਤਾ ਲਗਾਉਣਾ ਮੁਸ਼ਕਲ ਹੋ ਜਾਂਦਾ ਹੈ ਕਿ ਉਸ ਨਾਲ ਦੁਰਵਿਵਹਾਰ ਕੌਣ ਕਰ ਰਿਹਾ ਹੈ; ਸਾਈਬਰ ਬੁੱਲਿੰਗ

ਦੀ ਸਭ ਤੋਂ ਖਤਰਨਾਕ ਗੱਲ ਇਹ ਹੈ ਕਿ ਇਹ 24/7 ਹੋ ਸਕਦੀ ਹੈ—ਅਰਥਾਤ ਪੀੜਤ ਲਈ ਇਸ ਤੋਂ ਬਚਣਾ ਅਕਸਰ ਸੰਭਵ ਨਹੀਂ ਹੁੰਦਾ, ਕਿਉਂਕਿ ਡਿਜਿਟਲ ਡਿਵਾਈਸ ਹਮੇਸ਼ਾਂ ਉਸਦੇ ਨਾਲ ਹੁੰਦੇ ਹਨ; ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਹਿੰਸਾ ਬੱਚਿਆਂ, ਨੌਜਵਾਨਾਂ, ਬਾਲਗਾਂ—ਹਰੇਕ ਉਮਰ ਦੇ ਲੋਕਾਂ ਤੇ ਮਨੋਵਿਗਿਆਨਕ ਪ੍ਰਭਾਵ ਛੱਡ ਸਕਦੀ ਹੈ, ਜਿਵੇਂ ਕਿ anxiety, depression, low self-esteem, fear, stress ਅਤੇ ਕਈ ਵਾਰ self-harm ਤੱਕ ਦੇ ਖਤਰੇ ਪੈਦਾ ਹੋ ਸਕਦੇ ਹਨ; ਇਸ ਤੋਂ ਬਿਨਾਂ, cyber bullying ਦੀ ਵਜ੍ਹਾ ਨਾਲ ਪੀੜਤ ਅਕਸਰ ਸਮਾਜਿਕ ਤੌਰ 'ਤੇ ਅਲੱਗ ਹੋ ਜਾਂਦਾ ਹੈ, ਆਪਣੀ ਅਸਲੀਅਤ 'ਤੇ ਸ਼ੱਕ ਕਰਨ ਲੱਗਦਾ ਹੈ ਅਤੇ ਉਸਦੀ ਰੋਜ਼ਾਨਾ ਜ਼ਿੰਦਗੀ, ਪੜ੍ਹਾਈ ਜਾਂ ਨੌਕਰੀ 'ਤੇ ਵੀ ਨਕਾਰਾਤਮਕ ਪ੍ਰਭਾਵ ਪੈਂਦਾ ਹੈ; ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਸਿਰਫ਼ ਨਿੱਜੀ ਪੱਧਰ ਤੱਕ ਸੀਮਿਤ ਨਹੀਂ ਰਹਿੰਦੀ, ਕਈ ਵਾਰ ਇਹ ਜਨਤਕ ਤੌਰ 'ਤੇ ਵਾਇਰਲ ਹੋ ਕੇ ਪੀੜਤ ਨੂੰ ਹੋਰ ਵੱਡੀ ਤਕਲੀਫ਼ ਪੁੰਚਾ ਸਕਦੀ ਹੈ; ਇਸ ਦੇ ਕਾਰਣਾਂ ਵਿੱਚ jealousy, attention-seeking, revenge, group pressure ਜਾਂ ਕਿਸੇ ਦੇ ਉੱਪਰ ਹਕੂਮਤ ਕਰਨ ਦੀ ਮਨੋਵਿਰਤੀ ਸ਼ਾਮਲ ਹੁੰਦੀ ਹੈ; ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਨੂੰ ਰੋਕਣ ਅਤੇ ਘਟਾਉਣ ਲਈ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ, ਡਿਜਿਟਲ literacy, responsible online behaviour ਅਤੇ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਦੀ ਸਹੀ ਵਰਤੋਂ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ; ਇਸ ਨਾਲ ਨਾਲ ਪੀੜਤ ਲਈ ਇਹ ਵੀ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਬੁਲੀਅਰ ਦੇ ਨਾਲ direct contact ਤੋਂ ਬਚੇ, ਸਾਰੇ evidence ਸੰਭਾਲੇ, ਬੁਲੀਅਰ ਨੂੰ block ਕਰੇ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮ ਜਾਂ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਅਧਿਕਾਰੀਆਂ ਨੂੰ ਇਸ ਦੀ ਤੁਰੰਤ ਰਿਪੋਰਟ ਕਰੇ; ਸਮਾਜ, ਪਰਿਵਾਰ, ਸਕੂਲ ਅਤੇ ਤਕਨੀਕੀ ਪਲੇਟਫਾਰਮ ਸਭ ਮਿਲ ਕੇ ਜਾਗਰੂਕਤਾ ਨੂੰ ਵਧਾਉਣ ਅਤੇ cyber bullying ਦੇ ਖ਼ਿਲਾਫ਼ ਸਖ਼ਤ ਕਦਮ ਚੁੱਕਣਗੇ, ਤਾਂ ਹੀ ਡਿਜਿਟਲ ਦੁਨੀਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਇਆ ਜਾ ਸਕਦਾ ਹੈ।

ਉਦਾਹਰਨਾਂ

ਉਦਾਹਰਨ 1: ਧਮਕੀ ਭਰੇ ਮੈਸੇਜ ਭੇਜਣੇ

ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦਾ ਇੱਕ ਆਮ ਉਦਾਹਰਨ ਹੈ ਕਿਸੇ ਵਿਅਕਤੀ ਨੂੰ ਸੋਸ਼ਲ ਮੀਡੀਆ, WhatsApp, ਇਮੇਲ ਜਾਂ ਗੇਮਿੰਗ ਚੈਟ ਰਾਹੀਂ ਧਮਕੀ ਭਰੇ ਮੈਸੇਜ ਭੇਜਣਾ। ਉਦਾਹਰਨ ਲਈ, ਇੱਕ ਵਿਦਿਆਰਥੀ ਨੂੰ ਉਸਦੇ ਕਲਾਸਮੇਟ ਵੱਲੋਂ ਬਾਰ-ਬਾਰ “ਜੇ ਤੂੰ ਮੇਰੀ ਗੱਲ ਨਹੀਂ ਮੰਨਿਆ ਤਾਂ ਮੈਂ ਤੇਰੀਆਂ ਫੋਟੋਆਂ ਸਾਰੇ ਗਰੁੱਪ ਵਿੱਚ ਪਾ ਦਿਆਂਗਾ” ਜਾਂ “ਤੂੰ ਸਕੂਲ ਨਾ ਆਈਂ ਨਹੀਂ ਤਾਂ ਬੁਰਾ ਹੋਵੇਗਾ” ਜਿਹੇ ਮੈਸੇਜ ਮਿਲਣ ਲੱਗਦੇ ਹਨ। ਇਹ ਮੈਸੇਜ ਪੀੜਤ ਦੇ ਮਨ ਵਿੱਚ ਡਰ, ਗਲਤਫਹਿਮੀ ਅਤੇ ਤਣਾਅ ਪੈਦਾ ਕਰਦੇ ਹਨ। ਅਕਸਰ ਬੁਲੀਅਰ ਫੇਕ ਨੰਬਰ ਜਾਂ anonymous account ਵਰਤਦਾ ਹੈ, ਜਿਸ ਕਰਕੇ ਪਤਾ ਲਗਾਉਣਾ ਵੀ ਮੁਸ਼ਕਲ ਹੋ ਜਾਂਦਾ ਹੈ ਕਿ ਧਮਕੀਆਂ ਦੇਣ ਵਾਲਾ ਕੌਣ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਪੀੜਤ ਦੀ ਮਾਨਸਿਕ ਸਿਹਤ 'ਤੇ ਬਹੁਤ ਗੰਭੀਰ ਪ੍ਰਭਾਵ ਛੱਡ ਸਕਦੀ ਹੈ, ਉਹ ਡਰ ਦੇ ਮਾਰੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਵਰਤਣਾ ਵੀ ਛੱਡ ਸਕਦਾ ਹੈ।

ਉਦਾਹਰਨ 2: ਬਿਨਾਂ ਇਜਾਜ਼ਤ ਨਿੱਜੀ ਫੋਟੋਆਂ ਜਾਂ ਵੀਡੀਓ ਵਾਇਰਲ ਕਰਨਾ

ਇਹ ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਦਾ ਸਭ ਤੋਂ ਤਕਲੀਫ਼ਦੇਹ ਰੂਪ ਹੈ। ਉਦਾਹਰਨ ਲਈ, ਇੱਕ ਕੁੜੀ ਨੇ ਆਪਣੇ ਦੇਸਤ 'ਤੇ ਭਰੋਸਾ ਕਰਦੇ ਹੋਏ ਇੱਕ ਨਿੱਜੀ ਫੋਟੋ ਭੇਜੀ। ਬਾਅਦ ਵਿੱਚ ਜਦੋਂ ਝਗੜਾ ਹੋ ਗਿਆ, ਉਸ ਦੇਸਤ ਨੇ ਬਦਲਾ ਲੈਣ ਲਈ ਉਹ ਫੋਟੋ Snapchat, Instagram ਜਾਂ WhatsApp ਗਰੁੱਪਾਂ ਵਿੱਚ ਸ਼ੇਅਰ ਕਰ ਦਿੱਤੀ। ਇੱਕ ਛੋਟੀ ਜਿਹੀ ਫੋਟੋ ਪਲਾਂ ਵਿੱਚ ਸੈਂਕੜਿਆਂ ਲੋਕਾਂ ਤੱਕ ਪਹੁੰਚ ਜਾਂਦੀ ਹੈ ਅਤੇ ਪੀੜਤ ਨੂੰ ਸ਼ਰਮਿੰਦਗੀ, depression ਅਤੇ anxiety ਵਰਗੀਆਂ ਸਮੱਸਿਆਵਾਂ ਦਾ ਸਾਹਮਣਾ ਕਰਨਾ ਪੈਂਦਾ ਹੈ। ਕਈ ਵਾਰ ਲੋਕ comments ਕਰਕੇ ਮਖੌਲ ਉਡਾਉਂਦੇ ਹਨ, memes ਬਣਾਉਂਦੇ ਹਨ ਜਾਂ ਉਸਨੂੰ ਦੇਸ਼ੀ ਤਰ੍ਹਾਂ ਪੇਸ਼ ਕਰਦੇ ਹਨ। ਇਹ ਸਥਿਤੀ ਪੀੜਤ ਦੀ social reputation ਅਤੇ mental health ਦੇਵਾਂ ਨੂੰ ਬੁਰੀ ਤਰ੍ਹਾਂ ਪ੍ਰਭਾਵਿਤ ਕਰਦੀ ਹੈ।



ਉਦਾਹਰਨ 3: ਫੇਕ ਪ੍ਰੋਫਾਈਲ ਬਣਾਕੇ ਕਿਸੇ ਦੀ ਬਦਨਾਮੀ ਕਰਨਾ

ਕਈ ਬੁਲੀਅਰ ਕਿਸੇ ਵਿਅਕਤੀ ਦੇ ਨਾਮ, ਫੋਟੋ ਅਤੇ ਹੋਰ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਉਸਦੀ ਨਕਲੀ ਪ੍ਰੋਫਾਈਲ ਤਿਆਰ ਕਰ ਲੈਂਦੇ ਹਨ। ਉਦਾਹਰਨ ਲਈ, ਕਿਸੇ ਵਿਦਿਆਰਥੀ ਦੀ ਨਕਲੀ Facebook ਜਾਂ Instagram ID ਬਣਾਈ ਜਾ ਸਕਦੀ ਹੈ, ਜਿਸ 'ਤੇ ਅਪਮਾਨਜਨਕ ਪੋਸਟਾਂ, ਗੱਲਾਂ ਜਾਂ photos ਅਪਲੋਡ ਕੀਤੀਆਂ ਜਾਂਦੀਆਂ ਹਨ ਜਿਹਨਾਂ ਨਾਲ ਪੀੜਤ ਦੀ image ਖਰਾਬ ਹੋਵੇ। ਲੋਕ ਸਮਝਦੇ ਹਨ ਕਿ ਇਹ ਪੋਸਟਾਂ ਸੱਚਮੁੱਚ ਉਸੇ ਵਿਅਕਤੀ ਨੇ ਕੀਤੀਆਂ ਹਨ, ਜਿਸ ਨਾਲ

ਉਸਦੀ social reputation ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਦਾ ਹੈ। ਇਹ ਕਿਸਮ ਦੀ ਬੁੱਲਿੰਗ ਬਹੁਤ ਖਤਰਨਾਕ ਹੈ ਕਿਉਂਕਿ ਇਹ ਪੀੜਤ ਦੇ ਦੋਸਤਾਂ, ਪਰਿਵਾਰ ਅਤੇ ਅਧਿਆਪਕਾਂ ਵਿੱਚ ਗਲਤਫਹਿਮੀਆਂ ਪੈਦਾ ਕਰਦੀ ਹੈ। ਕਈ ਵਾਰ ਫੇਕ ਪ੍ਰੋਫਾਈਲ ਰਾਹੀਂ ਬੁਲੀਅਰ ਹੋਰ ਲੋਕਾਂ ਨੂੰ ਵੀ ਤੰਗ ਕਰਦਾ ਹੈ, ਜਿਸਦਾ ਦੇਸ਼ ਬੇਗੁਨਾਹ ਪੀੜਤ ਦੇ ਸਿਰ ਆ ਜਾਂਦਾ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਪੀੜਤ ਨੂੰ ਤਣਾਅ ਅਤੇ ਸ਼ਰਮਿੰਦਗੀ 'ਚ ਧੱਕ ਦਿੰਦੀ ਹੈ।

ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਇਸ ਤੋਂ ਬਚਾਅ ਦੇ ਤਰੀਕੇ

ਸਾਈਬਰ ਬੁੱਲਿੰਗ ਤੋਂ ਬਚਾਅ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਆਪਣੀਆਂ ਆਨਲਾਈਨ ਪ੍ਰਾਈਵੇਸੀ ਸੈਟਿੰਗਾਂ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਉਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ ਤਾਂ ਜੋ ਤੁਹਾਡੀਆਂ ਪੋਸਟਾਂ, ਫੋਟੋਆਂ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਿਰਫ਼ ਭਰੋਸੇਯੋਗ ਲੋਕਾਂ ਤੱਕ ਹੀ ਸੀਮਿਤ ਰਹੇ; ਅਣਜਾਣ ਲੋਕਾਂ ਦੀ friend request ਜਾਂ follow request ਕਦੇ ਵੀ ਨਾ ਸਵੀਕਾਰੋ ਅਤੇ ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ link, message ਜਾਂ profile ਨਾਲ engagement ਕਰਨ ਤੋਂ ਬਚੋ; ਆਪਣੇ ਪਾਸਵਰਡ ਮਜ਼ਬੂਤ ਅਤੇ unique ਬਣਾਓ ਅਤੇ ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA) ਦੀ ਵਰਤੋਂ ਕਰੋ ਤਾਂ ਜੋ ਕੋਈ ਤੁਹਾਡੇ account ਨੂੰ hack ਕਰਕੇ ਤੁਹਾਡਾ ਗਲਤ ਫਾਇਦਾ ਨਾ ਚੁੱਕ ਸਕੇ; ਜੇ ਕਿਸੇ ਵਲੋਂ ਤੁਹਾਨੂੰ ਅਪਮਾਨਜਨਕ, ਧਮਕੀ ਭਰੇ ਜਾਂ ਤੰਗ ਕਰਨ ਵਾਲੇ ਮੈਸੇਜ ਮਿਲਣ, ਤਾਂ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਉਸ ਵਿਅਕਤੀ ਨੂੰ block ਕਰੋ ਅਤੇ ਉਸਦੇ ਮੈਸੇਜਾਂ ਦੇ screenshots ਜਾਂ records ਸੰਭਾਲ ਕੇ ਰੱਖੋ, ਕਿਉਂਕਿ ਇਹ evidence ਰਿਪੋਰਟ ਕਰਨ ਵੇਲੇ ਕੰਮ ਆਉਂਦਾ ਹੈ; ਬੁਲੀਅਰ ਨੂੰ ਕਦੇ ਵੀ reply ਨਾ ਕਰੋ ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਉਹ ਹੋਰ ਹੌਸਲਾ ਪਾ ਸਕਦਾ ਹੈ; ਇਸ ਤੋਂ ਬਾਅਦ ਉਸ incident ਨੂੰ ਤੁਰੰਤ ਆਪਣੇ ਮਾਪਿਆਂ, ਅਧਿਆਪਕਾਂ ਜਾਂ ਕਿਸੇ ਭਰੋਸੇਯੋਗ ਵੱਡੇ ਵਿਅਕਤੀ ਨੂੰ ਦੱਸੋ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮ ਦੇ “Report” option ਰਾਹੀਂ ਉਸ ਬੁਲੀਅਰ ਦੀ complaint ਦਿਓ; ਜੇ ਮਾਮਲਾ ਗੰਭੀਰ ਜਾਂ ਖਤਰਨਾਕ ਹੋਵੇ, ਤਾਂ ਸਾਈਬਰ ਸੈੱਲ ਜਾਂ ਕਾਨੂੰਨੀ ਅਧਿਕਾਰੀਆਂ ਨੂੰ ਰਿਪੋਰਟ ਕਰਨਾ ਸਭ ਤੋਂ ਸੁਰੱਖਿਅਤ ਤਰੀਕਾ ਹੈ;

ਇਸਦੇ ਨਾਲ ਹੀ, ਡਿਜਿਟਲ ਲਿਟਰੇਸੀ ਵਧਾਉਂਦੇ ਹੋਏ ਜ਼ਿੰਮੇਵਾਰ ਆਨਲਾਈਨ ਵਰਤੋਂ ਦੀ ਆਦਤ ਬਣਾਓ, ਕੋਈ ਭੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਬਿਨਾਂ ਸੋਚੇ ਸਮਝੇ share ਨਾ ਕਰੋ ਅਤੇ ਆਪਣੇ ਦੋਸਤਾਂ ਨੂੰ ਵੀ ਸਾਈਬਰ ਬੁਲਿੰਗ ਦੇ ਖਤਰੇ ਅਤੇ ਬਚਾਅ ਬਾਰੇ ਜਾਗਰੂਕ ਕਰੋ ਤਾਂ ਜੋ ਇੱਕ ਸੁਰੱਖਿਅਤ ਡਿਜਿਟਲ ਵਾਤਾਵਰਣ ਤਿਆਰ ਕੀਤਾ ਜਾ ਸਕੇ।

ਕਿੱਦਾਂ ਰਿਪੋਰਟ ਕਰਨਾ ਹੈ (Parents, Teachers, Police/Helpline)

ਸਾਈਬਰ ਬੁਲਿੰਗ ਉਹ ਹਰਕਤ ਹੈ ਜਿਸ ਵਿੱਚ ਕਿਸੇ ਨੂੰ ਆਨਲਾਈਨ ਤਰ੍ਹਾਂ ਤੰਗ ਕੀਤਾ ਜਾਂਦਾ ਹੈ—ਜਿਵੇਂ ਕਿ ਬੁਰੇ ਸੁਨੇਹੇ ਭੇਜਣ, ਫਰਜ਼ੀ ਖਾਤੇ ਬਣਾਉਣ, ਧਮਕੀ ਦੇਣ, ਫੋਟੋ/ਵੀਡੀਓ ਬਲੈਕਮੇਲ ਲਈ ਵਰਤਨਾ, ਜਾਂ ਕਿਸੇ ਦੀ ਬੇਇਜ਼ਤੀ ਕਰਨਾ। ਜੇ ਤੁਹਾਡੇ ਨਾਲ ਜਾਂ ਤੁਹਾਡੇ ਜਾਣਕਾਰ ਕਿਸੇ ਨਾਲ ਸਾਈਬਰ ਬੁਲਿੰਗ ਹੋ ਰਹੀ ਹੈ, ਤਾਂ ਉਸਦੀ ਸ਼ਿਕਾਇਤ ਕਰਨੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।



1. ਸਬੂਤ ਸੰਭਾਲੋ

ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਉਸ ਬੁਲਿੰਗ ਦੇ ਸਬੂਤ ਜਿਵੇਂ—ਸਕਰੀਨਸ਼ਾਟ, ਚੈਟ ਰਿਕਾਰਡ, ਈਮੇਲ, ਟਿੱਪਣੀਆਂ, ਜਾਂ ਫੋਟੋ/ਵੀਡੀਓ—ਸੰਭਾਲ ਕੇ ਰੱਖੋ। ਸਬੂਤ ਸ਼ਿਕਾਇਤ ਦੌਰਾਨ ਬਹੁਤ ਮਦਦ ਕਰਦੇ ਹਨ।

2. ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮ 'ਤੇ ਰਿਪੋਰਟ ਕਰੋ

ਜ਼ਿਆਦਾਤਰ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੇਟਫਾਰਮ (Facebook, Instagram, YouTube, WhatsApp, Snapchat) ਸਾਈਬਰ ਬੁਲਿੰਗ ਜਾਂ ਹੋਟ ਸਮੱਗਰੀ ਨੂੰ ਰਿਪੋਰਟ ਕਰਨ ਦਾ ਵਿਕਲਪ ਦਿੰਦੇ ਹਨ।

- “Report” ਬਟਨ ਤੇ ਕਲਿੱਕ ਕਰੋ
- ਸਬੂਤ ਜਾਂ ਕਾਰਨ ਦੱਸੋ

- ਪਲੇਟਫਾਰਮ ਅਕਸਰ 24-48 ਘੰਟਿਆਂ ਵਿੱਚ ਕਾਰਵਾਈ ਕਰਦਾ ਹੈ

ਇਸਦੇ ਨਾਲ-ਨਾਲ ਉਸ ਯੂਜ਼ਰ ਨੂੰ ਬਲੋਕ ਕਰਨਾ ਵੀ ਚਾਹੀਦਾ ਹੈ।

3. ਪੰਜਾਬ ਪੁਲਿਸ ਦੀ ਸਾਈਬਰ ਸੈੱਲ ਨੂੰ ਸ਼ਿਕਾਇਤ ਕਰੋ

ਭਾਰਤ ਵਿੱਚ ਹਰ ਰਾਜ ਵਿੱਚ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਸੈੱਲ ਹੁੰਦਾ ਹੈ। ਤੁਸੀਂ:

- ਨਜ਼ਦੀਕੀ ਸਾਈਬਰ ਸੈੱਲ ਦਫ਼ਤਰ ਜਾ ਕੇ ਸ਼ਿਕਾਇਤ ਕਰ ਸਕਦੇ ਹੋ
- ਜਾਂ National Cyber Crime Reporting Portal <http://www.cybercrime.gov.in> 'ਤੇ ਆਨਲਾਈਨ ਸ਼ਿਕਾਇਤ ਦੇ ਸਕਦੇ ਹੋ

ਇੱਥੇ ਤੁਸੀਂ “Women/Child Related Crimes” ਜਾਂ “Cyber Bullying” ਸ਼੍ਰੇਣੀ ਚੁਣ ਕੇ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰ ਸਕਦੇ ਹੋ।

ਇਸ ਤੋਂ ਇਲਾਵਾ ਤੁਸੀਂ “Child Related Crimes” ਜਾਂ “Cyber Bullying” ਸਬੰਧੀ Child Right Commission ਦੇ ਟੈਲ ਫਰੀ ਨੰਬਰ 1098 ਤੇ ਵੀ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰ ਸਕਦੇ ਹੋ।

4. ਸਕੂਲ/ਕਾਲਜ ਜਾਂ ਕੰਮ ਕਰਨ ਵਾਲੀ ਥਾਂ 'ਤੇ ਦੱਸੋ

ਜੇ ਸਾਈਬਰ ਬੁਲਿੰਗ ਵਿਦਿਆਰਥੀਆਂ ਵਿਚਾਲੇ ਹੋ ਰਹੀ ਹੈ ਤਾਂ ਅਧਿਆਪਕਾਂ, ਸਕੂਲ ਪ੍ਰਬੰਧਨ ਜਾਂ ਕੌਂਸਲਰ ਨੂੰ ਤੁਰੰਤ ਦੱਸਣਾ ਚਾਹੀਦਾ ਹੈ। ਕੰਮ ਵਾਲੀ ਥਾਂ 'ਤੇ ਇਹ HR ਜਾਂ ਸੁਰੱਖਿਆ ਵਿਭਾਗ ਨੂੰ ਦੱਸਿਆ ਜਾ ਸਕਦਾ ਹੈ।

5. ਕਾਨੂੰਨੀ ਕਾਰਵਾਈ

ਭਾਰਤੀ ਕਾਨੂੰਨ (IT Act 2000, IPC Sections 354D, 506, 509) ਸਾਈਬਰ ਬੁਲਿੰਗ, ਸਟਾਕਿੰਗ ਅਤੇ ਧਮਕੀ ਦੇਣ 'ਤੇ ਸਖ਼ਤ ਸਜ਼ਾਵਾਂ ਦਾ ਪ੍ਰਬੰਧ ਕਰਦੇ ਹਨ। ਜ਼ਰੂਰਤ ਹੋਣ 'ਤੇ FIR ਵੀ ਦਰਜ ਕਰਵਾਈ ਜਾ ਸਕਦੀ ਹੈ।

ਸਾਈਬਰ ਬੁਲਿੰਗ ਨੂੰ ਕਦੇ ਵੀ ਹਲਕਾ ਨਾ ਲਓ। ਸਮੇਂ 'ਤੇ ਸ਼ਿਕਾਇਤ ਕਰਨਾ ਆਪਣੇ ਆਪ ਨੂੰ ਅਤੇ ਹੋਰਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਦਾ ਸਭ ਤੋਂ ਵਧੀਆ ਤਰੀਕਾ ਹੈ।

5. ਫਿਸ਼ਿੰਗ ਠੱਗੀ ਕੀ ਹੈ? ਇਸ ਤੋਂ ਬਚਾਅ ਦੇ ਤਰੀਕੇ

1. ਫਿਸ਼ਿੰਗ (Phishing)

ਫਿਸ਼ਿੰਗ ਇੱਕ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਤਰੀਕਾ ਹੈ ਜਿਸ ਵਿੱਚ ਠੱਗ ਲੋਕ ਨਕਲੀ ਈਮੇਲਾਂ, ਨਕਲੀ ਵੈਬਸਾਈਟਾਂ ਜਾਂ ਨਕਲੀ ਸੰਦੇਸ਼ਾਂ ਰਾਹੀਂ ਯੂਜ਼ਰਾਂ ਨੂੰ ਧੋਖਾ ਦੇ ਕੇ ਉਨ੍ਹਾਂ ਦੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਪਾਸਵਰਡ, ਬੈਂਕ ਖਾਤਾ ਨੰਬਰ, ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਡੀਟੇਲ, ਆਧਾਰ ਨੰਬਰ ਜਾਂ ਹੋਰ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਲੈਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦੇ ਹਨ। ਇਹ ਅਕਸਰ ਕਿਸੇ ਭਰੋਸੇਮੰਦ ਸੰਸਥਾ ਦਾ ਨਾਂ ਵਰਤਦੇ ਹਨ — ਜਿਵੇਂ ਬੈਂਕ, ਸਰਕਾਰੀ ਵਿਭਾਗ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਵੈਬਸਾਈਟ ਜਾਂ ਕੋਈ ਕੰਪਨੀ। ਫਿਸ਼ਿੰਗ ਈਮੇਲ ਅਕਸਰ ਇਸ ਤਰ੍ਹਾਂ ਦੇ ਲਿਖੇ ਹੁੰਦੇ ਹਨ ਕਿ ਯੂਜ਼ਰ ਨੂੰ ਲੱਗੇ ਕਿ ਇਹ ਸਹੀ ਸਰੋਤ ਤੋਂ ਆਏ ਹਨ। ਉਹ ਈਮੇਲ ਵਿੱਚ ਇੱਕ ਲਿੰਕ ਹੁੰਦਾ ਹੈ ਜੋ ਇੱਕ ਨਕਲੀ ਵੈਬਸਾਈਟ 'ਤੇ ਲੈ ਜਾਂਦਾ ਹੈ ਜੋ ਦਿਖਣ ਵਿੱਚ ਬਿਲਕੁਲ ਅਸਲੀ ਵੈਬਸਾਈਟ ਵਰਗੀ ਹੀ ਹੁੰਦੀ ਹੈ। ਜਦੋਂ ਯੂਜ਼ਰ ਉਸ ਵੈਬਸਾਈਟ 'ਤੇ ਆਪਣੀ ਜਾਣਕਾਰੀ ਭਰਦਾ ਹੈ, ਤਾਂ ਉਹ ਸਾਰੀ ਡੀਟੇਲ ਸਿੱਧੀ ਠੱਗਾਂ ਦੇ ਹੱਥ ਲੱਗ ਜਾਂਦੀ ਹੈ। ਫਿਸ਼ਿੰਗ ਦਾ ਉਦੇਸ਼ ਪੈਸਾ ਚੁਰਾਉਣਾ, ਖਾਤੇ ਹੈਕ ਕਰਨਾ, ਪਛਾਣ ਚੋਰੀ ਕਰਨਾ ਜਾਂ ਹੋਰ ਕਿਸਮ ਦੇ ਸਾਈਬਰ ਅਪਰਾਧ ਕਰਨਾ ਹੁੰਦਾ ਹੈ। ਫਿਸ਼ਿੰਗ ਤੋਂ ਬਚਣ ਲਈ ਸਹੀ ਸਰੋਤ ਦੀ ਜਾਂਚ ਕਰਨੀ, ਸ਼ੱਕੀ ਈਮੇਲਾਂ ਨਾ ਖੋਲ੍ਹਣੀਆਂ, ਅਣਜਾਣ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨਾ ਅਤੇ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਤਰੀਕਿਆਂ ਦੀ ਪਾਲਣਾ ਕਰਨੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੁੰਦੀ ਹੈ।



2. ਸਮਿਸ਼ਿੰਗ (Smishing)

ਸਮਿਸ਼ਿੰਗ ਫਿਸ਼ਿੰਗ ਦੀ ਇੱਕ ਰੂਪ-ਬਦਲੀ ਹੋਈ ਸ਼ੈਲ ਹੈ ਜਿਸ ਵਿੱਚ ਠੱਗ ਲੋਕ ਈਮੇਲ ਦੀ ਬਜਾਏ SMS (ਟੈਕਸਟ ਮੈਸੇਜ) ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। “Smishing” ਵਿੱਚ “SMS” ਅਤੇ “Phishing” ਦੇ ਸ਼ਬਦ ਮਿਲ ਕੇ ਬਣਦੇ ਹਨ। ਸਮਿਸ਼ਿੰਗ ਹਮਲਿਆਂ ਵਿੱਚ ਠੱਗ ਕੋਈ ਨਕਲੀ SMS ਭੇਜਦੇ ਹਨ ਜਿਸ ਵਿੱਚ ਆਮ ਤੌਰ 'ਤੇ ਲਿਖਿਆ ਹੁੰਦਾ ਹੈ ਕਿ ਤੁਹਾਡਾ ਬੈਂਕ ਖਾਤਾ ਬਲੌਕ ਹੋ ਗਿਆ ਹੈ, ਤੁਹਾਨੂੰ ਕੋਈ ਇਨਾਮ ਮਿਲਿਆ ਹੈ, ਤੁਹਾਡੀ ਡਿਲੀਵਰੀ ਰੁਕੀ ਹੋਈ ਹੈ ਜਾਂ ਤੁਸੀਂ ਕੋਈ ਲਿੰਕ ਖੋਲ੍ਹਕੇ ਆਪਣੀ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ। ਇਹ SMS ਲੋਕਾਂ ਨੂੰ ਘਬਰਾ ਕੇ ਜਾਂ ਲਾਲਚ ਦੇ ਕੇ ਕਿਸੇ ਨਕਲੀ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਲਈ ਮਜਬੂਰ ਕਰਦੇ ਹਨ। ਜਦੋਂ ਯੂਜ਼ਰ ਉਹ ਲਿੰਕ ਖੋਲ੍ਹਦਾ ਹੈ, ਤਾਂ ਉਹ ਇੱਕ ਨਕਲੀ ਵੈਬਸਾਈਟ 'ਤੇ ਪਹੁੰਚਦਾ ਹੈ ਜਾਂ ਉਸਦੇ ਫੋਨ ਵਿੱਚ ਮਾਲਵੇਅਰ ਇੰਸਟਾਲ ਹੋ ਸਕਦਾ ਹੈ, ਜਿਸ ਰਾਹੀਂ ਠੱਗਾਂ ਨੂੰ ਪਾਸਵਰਡ, ਬੈਂਕਿੰਗ ਜਾਣਕਾਰੀ ਜਾਂ ਫੋਨ ਡਾਟਾ ਤੱਕ ਪਹੁੰਚ ਮਿਲ ਜਾਂਦੀ ਹੈ। ਕਈ ਵਾਰ ਸਮਿਸ਼ਿੰਗ ਵਿੱਚ ਠੱਗ SMS ਰਾਹੀਂ ਯੂਜ਼ਰ ਨੂੰ ਕਾਲ ਕਰਨ ਲਈ ਵੀ ਕਹਿ ਦਿੰਦੇ ਹਨ, ਤਾਂ ਜੋ ਉਹ ਉਸ ਤੋਂ ਸਿੱਧੀ ਜਾਣਕਾਰੀ ਹਾਸਲ ਕਰ ਸਕਣ। ਸਮਿਸ਼ਿੰਗ ਤੋਂ ਬਚਣ ਲਈ ਅਣਜਾਣ ਨੰਬਰਾਂ ਦੇ ਮੈਸੇਜਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹਿਣਾ, ਕਿਸੇ ਵੀ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨਾ, ਬੈਂਕ ਜਾਂ ਕੰਪਨੀ ਨਾਲ ਸਿੱਧਾ ਸੰਪਰਕ ਕਰਨਾ ਅਤੇ ਮੋਬਾਈਲ ਵਿੱਚ ਸੁਰੱਖਿਆ ਐਪ ਵਰਤਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

3. ਵਿਸ਼ਿੰਗ (Vishing)

ਵਿਸ਼ਿੰਗ ਇੱਕ ਸਾਈਬਰ ਠੱਗੀ ਤਰੀਕਾ ਹੈ ਜਿਸ ਵਿੱਚ ਠੱਗ ਲੋਕ **ਵੋਇਸ ਕਾਲ (Phone Call)** ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਨ। “Vishing” ਵਿੱਚ “Voice” ਅਤੇ “Phishing” ਸ਼ਬਦ ਮਿਲ ਕੇ ਬਣੇ ਹਨ। ਵਿਸ਼ਿੰਗ ਹਮਲਿਆਂ ਵਿੱਚ ਠੱਗ ਆਪਣੇ ਆਪ ਨੂੰ ਬੈਂਕ ਅਫਸਰ, ਸਰਕਾਰੀ ਅਧਿਕਾਰੀ, ਟੈਲੀਕਾਮ ਕੰਪਨੀ, ਇਨਸ਼ੋਰੈਂਸ ਅਜੰਟ ਜਾਂ ਕਿਸੇ ਹੋਰ ਭਰੋਸੇਮੰਦ ਸੰਸਥਾ ਦਾ ਕਾਰਿੰਦਾ ਦੱਸਦੇ ਹਨ।



ਉਹ ਕਹਿੰਦੇ ਹਨ ਕਿ ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਕੋਈ ਸਮੱਸਿਆ ਹੈ, KYC ਅਪਡੇਟ ਕਰਨੀ ਹੈ, ਤੁਹਾਡਾ ATM ਬਲੋਕ ਹੋ ਗਿਆ ਹੈ, ਜਾਂ ਕੋਈ ਸ਼ੱਕੀ ਲੈਣ-ਦੇਣ ਹੋਈ ਹੈ। ਇਸ ਤਰੀਕੇ ਨਾਲ ਉਹ ਯੂਜ਼ਰ ਤੋਂ OTP, ATM PIN, ਪਾਸਵਰਡ, ਖਾਤਾ ਨੰਬਰ ਜਾਂ ਹੋਰ ਗੁਪਤ ਜਾਣਕਾਰੀ ਲੈ ਲੈਂਦੇ ਹਨ। ਕੁਝ ਠੱਗ ਕਾਲਰ ID ਨੂੰ ਵੀ ਸਪੂਰਤ ਕਰਦੇ ਹਨ ਤਾਂ ਕਿ ਯੂਜ਼ਰ ਨੂੰ ਲੱਗੇ ਕਿ ਕਾਲ ਸੱਚਮੁੱਚ ਬੈਂਕ ਦੀ ਹੈ। ਵਿਸ਼ਿੰਗ ਦੇ ਠੱਗਾਂ ਦਾ ਮੁੱਖ ਉਦੇਸ਼ ਖਾਤਿਆਂ ਤੋਂ ਪੈਸਾ ਚੁਰਾਉਣਾ ਜਾਂ ਪਛਾਣ ਚੋਰੀ ਕਰਨਾ ਹੁੰਦਾ ਹੈ। ਵਿਸ਼ਿੰਗ ਤੋਂ ਬਚਣ ਲਈ ਹਮੇਸ਼ਾਂ ਯਾਦ ਰੱਖੋ ਕਿ ਕੋਈ ਵੀ ਬੈਂਕ ਜਾਂ ਸਰਕਾਰੀ ਸੰਸਥਾ ਕਦੇ ਵੀ OTP, PIN, ਅਤੇ ਪਾਸਵਰਡ ਫੋਨ 'ਤੇ ਨਹੀਂ ਮੰਗਦੀ। ਸ਼ੱਕੀ ਕਾਲਾਂ ਉੱਤੇ ਆਪਣੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰੋ, ਕਾਲ ਕੱਟ ਦਿਓ ਅਤੇ ਜੇ ਸੰਗਠਨ ਦਾ ਨਾਂ ਲਿਆ ਗਿਆ ਹੈ ਉਸ ਨਾਲ ਖੁਦ ਸੰਪਰਕ ਕਰੋ। ਸੁਰੱਖਿਆ ਲਈ ਹਮੇਸ਼ਾਂ ਸਚੇਤ ਅਤੇ ਸਾਵਧਾਨ ਰਹਿਣਾ ਸਭ ਤੋਂ ਵਧੀਆ ਤਰੀਕਾ ਹੈ।

ਫਰਾਡ ਲਿੰਕ, ਫੇਕ ਈ-ਮੇਲ, ਓਟੀਪੀ ਫਰਾਡ

1. Fraud Links (ਠੱਗੀ ਵਾਲੇ ਲਿੰਕ)

Fraud Links ਉਹ ਨਕਲੀ ਜਾਂ ਖਤਰਨਾਕ ਲਿੰਕ ਹੁੰਦੇ ਹਨ ਜੋ ਠੱਗ ਲੋਕ ਖਾਸ ਤੌਰ 'ਤੇ ਯੂਜ਼ਰਾਂ ਨੂੰ ਧੋਖਾ ਦੇਣ ਲਈ ਤਿਆਰ ਕਰਦੇ ਹਨ। ਇਹ ਲਿੰਕ ਆਮ ਤੌਰ 'ਤੇ SMS, WhatsApp, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਈਮੇਲ ਜਾਂ ਅਣਜਾਣ ਵੈਬਸਾਈਟਾਂ 'ਤੇ ਭੇਜੇ ਜਾਂਦੇ ਹਨ। ਇਹਨਾਂ ਦਾ ਮੁੱਖ ਉਦੇਸ਼ ਯੂਜ਼ਰ ਤੋਂ ਨਿੱਜੀ ਜਾਂ ਬੈਂਕਿੰਗ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਨਾ ਹੁੰਦਾ ਹੈ। ਅਕਸਰ ਇਹ ਲਿੰਕ ਕੋਈ ਆਕਰਸ਼ਕ ਪੇਸ਼ਕਸ਼, ਇਨਾਮ, ਡਿਸਕਾਊਂਟ, ਡਿਲੀਵਰੀ ਅਪਡੇਟ ਜਾਂ ਬੈਂਕ ਚੇਤਾਵਨੀ ਦੇ ਨਾਂ 'ਤੇ ਭੇਜੇ ਜਾਂਦੇ ਹਨ। ਜਦੋਂ ਯੂਜ਼ਰ ਉਹ ਲਿੰਕ ਖੋਲ੍ਹਦਾ ਹੈ, ਤਾਂ ਉਹ ਕਿਸੇ ਨਕਲੀ ਵੈਬਸਾਈਟ 'ਤੇ ਪਹੁੰਚਦਾ ਹੈ, ਜੋ ਦਿਖਣ ਵਿੱਚ ਬਿਲਕੁਲ ਅਸਲੀ ਵੈਬਸਾਈਟ ਵਰਗੀ ਲੱਗਦੀ ਹੈ। ਇਸ 'ਤੇ ਡਾਟਾ ਭਰਨ 'ਤੇ ਸਾਰੀ ਜਾਣਕਾਰੀ ਸੀਧੀ ਠੱਗ ਦੇ ਹੱਥ ਲੱਗ ਜਾਂਦੀ ਹੈ। ਕਈ ਵਾਰ ਇਹ ਲਿੰਕ ਖੋਲ੍ਹਣ ਨਾਲ ਯੂਜ਼ਰ ਦੇ ਫੋਨ ਜਾਂ ਕੰਪਿਊਟਰ ਵਿੱਚ ਮਾਲਵੇਅਰ, ਸਪਾਈਵੇਅਰ ਜਾਂ ਵਾਇਰਸ ਇੰਸਟਾਲ ਹੋ ਜਾਂਦਾ ਹੈ, ਜੋ ਡਿਵਾਈਸ ਦਾ ਡਾਟਾ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ। Fraud Links ਤੋਂ ਬਚਣ ਲਈ ਹਮੇਸ਼ਾਂ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਉਸਦੀ ਸਹੀਅਤਾ ਜਾਂਚੋ, ਅਣਜਾਣ ਸਰੋਤਾਂ ਦੇ ਮੇਸੇਜਾਂ ਨੂੰ ਨਜ਼ਰਅੰਦਾਜ਼ ਕਰੋ, ਵੈਬਸਾਈਟ ਦਾ ਐਡਰੈੱਸ ਦੇਖੋ ਅਤੇ ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਐਪਸ ਜਾਂ ਸਾਈਟਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ।

2. Fake Emails (ਨਕਲੀ ਈ-ਮੇਲ)

Fake Emails ਉਹ ਈਮੇਲ ਹਨ ਜੋ ਠੱਗ ਲੋਕ ਕਿਸੇ ਅਸਲੀ ਸੰਸਥਾ ਜਾਂ ਵਿਅਕਤੀ ਦੇ ਨਾਂ 'ਤੇ ਭੇਜਦੇ ਹਨ, ਤਾਂ ਜੋ ਯੂਜ਼ਰ ਤੋਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਪੈਸੇ ਜਾਂ ਲਾਗਇਨ ਡਾਟਾ ਹਾਸਲ ਕੀਤਾ ਜਾ ਸਕੇ। ਇਹ ਈਮੇਲ ਅਕਸਰ ਬੈਂਕ, ਸਰਕਾਰੀ ਦਫਤਰ, ਕੂਰੀਅਰ ਕੰਪਨੀ, ਜੈਬ ਆਫਰ ਜਾਂ ਇ-ਕਾਮਰਸ ਪਲਾਟਫਾਰਮ ਦਾ ਨਾਂ ਲੈ ਕੇ ਭੇਜੇ ਜਾਂਦੇ ਹਨ। ਇਹਨਾਂ ਵਿੱਚ ਅਕਸਰ ਲਿਖਿਆ ਹੁੰਦਾ ਹੈ ਕਿ ਤੁਹਾਡਾ ਖਾਤਾ ਬਲੋਕ ਹੋ ਗਿਆ ਹੈ, ਤੁਸੀਂ ਇਨਾਮ ਜਿੱਤਿਆ ਹੈ, KYC ਅਪਡੇਟ ਕਰਨੀ ਹੈ, ਜਾਂ ਤੁਹਾਨੂੰ ਬਿੱਲ ਭਰਨਾ ਹੈ। Fake Emails ਵਿੱਚ ਅਕਸਰ ਇੱਕ ਲਿੰਕ ਜਾਂ ਐਟੈਚਮੈਂਟ ਹੁੰਦਾ ਹੈ ਜੋ ਨਕਲੀ ਵੈਬਸਾਈਟ 'ਤੇ ਲੈ ਜਾਂਦਾ ਹੈ ਜਾਂ ਡਿਵਾਈਸ ਵਿੱਚ ਵਾਇਰਸ ਇੰਸਤਾਲ ਕਰਦਾ ਹੈ। ਇਹ ਈਮੇਲਾਂ ਅਸਲੀ ਈਮੇਲਾਂ ਵਰਗੀਆਂ ਹੀ ਦਿਖਦੀਆਂ ਹਨ, ਪਰ ਉਨ੍ਹਾਂ ਦੀ ਭਾਸ਼ਾ, ਭੇਜਣ ਵਾਲੇ ਦਾ ਪਤਾ ਅਤੇ ਲਿੰਕ ਦੀ ਮੰਜਿਲ ਗਲਤ ਹੁੰਦੀ ਹੈ। ਨਕਲੀ ਈਮੇਲ ਪਛਾਣਣ ਲਈ ਭੇਜਣ ਵਾਲੇ ਦਾ ਈਮੇਲ ਐਡਰੈੱਸ ਧਿਆਨ ਨਾਲ ਵੇਖੋ, ਗਲਤੀਆਂ ਵਾਲੇ ਵਾਕਾਂ ਨੂੰ ਪਛਾਣੋ, ਅਣਜਾਣ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ ਅਤੇ ਅਸਲੀ ਸੰਸਥਾ ਨਾਲ ਸਿੱਧਾ ਸੰਪਰਕ ਕਰੋ। Fake Emails ਦਾ ਉਦੇਸ਼ ਯੂਜ਼ਰ ਦਾ ਭਰੋਸਾ ਜਿੱਤ ਕੇ ਉਸ ਤੋਂ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਚੁਰਾਉਣਾ ਹੁੰਦਾ ਹੈ।

3. OTP Fraud (ਓਟੀਪੀ ਠੱਗੀ)

OTP Fraud ਉਹ ਠੱਗੀ ਹੈ ਜਿਸ ਵਿੱਚ ਅਪਰਾਧੀ ਯੂਜ਼ਰ ਤੋਂ OTP (One-Time Password) ਚੋਰੀ ਕਰਕੇ ਉਸਦੇ ਬੈਂਕ ਖਾਤੇ, ਡਿਜ਼ਿਟਲ ਵਾਲੇਟ ਜਾਂ ਹੋਰ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਵਿੱਚ ਘੁੱਸਦੇ ਹਨ। ਠੱਗ ਅਕਸਰ ਯੂਜ਼ਰ ਨੂੰ ਕਾਲ ਕਰਦੇ ਹਨ, ਆਪਣੇ ਆਪ ਨੂੰ ਬੈਂਕ ਅਫਸਰ, KYC ਏਜੰਟ, ਕਸਟਮਰ ਕੇਅਰ ਜਾਂ ਇੱਕ ਕੰਪਨੀ ਦਾ ਕਰਮਚਾਰੀ ਦੱਸਦੇ ਹਨ। ਉਹ ਕਹਿੰਦੇ ਹਨ ਕਿ ਤੁਹਾਡਾ KYC ਅਪਡੇਟ ਕਰਨਾ ਹੈ, ਖਾਤਾ ਬਲੋਕ ਹੋ ਰਿਹਾ ਹੈ, ਰਿਫੰਡ ਮਿਲਣਾ ਹੈ ਜਾਂ ਇਨਾਮ ਮਿਲਿਆ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਉਹ ਯੂਜ਼ਰ ਨੂੰ ਇਹ ਵਿਸ਼ਵਾਸ ਦਿਵਾਉਂਦੇ ਹਨ ਕਿ OTP ਸਾਂਝੀ ਕਰਨੀ ਜ਼ਰੂਰੀ ਹੈ, ਜਦਕਿ ਹਕੀਕਤ ਵਿੱਚ OTP ਸਿਰਫ ਯੂਜ਼ਰ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਹੁੰਦਾ ਹੈ ਅਤੇ ਕੋਈ ਵੀ ਅਧਿਕਾਰਿਤ ਸੰਸਥਾ ਕਦੇ ਵੀ ਇਸਦੀ ਮੰਗ ਨਹੀਂ ਕਰਦੀ। ਜਿਵੇਂ ਹੀ ਯੂਜ਼ਰ OTP ਦਿੰਦਾ ਹੈ, ਠੱਗ ਟ੍ਰਾਂਜੈਕਸ਼ਨ ਪੂਰੀ ਕਰਦੇ ਹਨ ਅਤੇ ਖਾਤੇ ਤੋਂ ਪੈਸਾ ਕੱਢ ਲੈਂਦੇ ਹਨ। ਕਈ ਵਾਰ ਠੱਗ ਨਕਲੀ ਲਿੰਕ ਭੇਜ ਕੇ ਲਾਗਇਨ ਕਰਨ ਲਈ ਕਹਿੰਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਫੇਨ 'ਤੇ OTP ਆ ਜਾਂਦਾ ਹੈ ਅਤੇ ਯੂਜ਼ਰ ਨੂੰ ਧੋਖਾ ਦੇ ਕੇ ਉਹ OTP ਹਾਸਲ ਕਰ ਲੈਂਦੇ ਹਨ। OTP Fraud ਤੋਂ ਬਚਣ ਲਈ ਹਮੇਸ਼ਾਂ ਯਾਦ ਰੱਖੋ ਕਿ OTP ਕਿਸੇ ਨਾਲ ਵੀ ਸਾਂਝਾ ਨਾ ਕਰੋ, ਕਿਸੇ ਕਾਲ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ, ਬੈਂਕ ਨਾਲ ਸਿੱਧਾ ਸੰਪਰਕ ਕਰੋ ਅਤੇ ਸ਼ੱਕੀ ਲਿੰਕ ਨਾ ਖੋਲ੍ਹੋ।

ਅਣਜਾਣ ਲਿੰਕਾਂ ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨਾ

ਅਣਜਾਣ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨਾ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਲਈ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਨਿਯਮਾਂ ਵਿੱਚੋਂ ਇੱਕ ਹੈ, ਕਿਉਂਕਿ ਇੰਟਰਨੈੱਟ 'ਤੇ ਬਹੁਤ ਸਾਰੇ ਠੱਗ ਨਕਲੀ, ਖਤਰਨਾਕ ਜਾਂ ਧੋਖੇਬਾਜ਼ੀ ਵਾਲੇ ਲਿੰਕ ਭੇਜਦੇ ਹਨ ਜੋ ਯੂਜ਼ਰਾਂ ਦੇ ਡਾਟਾ, ਬੈਂਕ ਖਾਤਿਆਂ ਜਾਂ ਡਿਵਾਈਸਾਂ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਲਈ ਬਣਾਏ ਜਾਂਦੇ ਹਨ। ਇਹ ਲਿੰਕ ਅਕਸਰ SMS, WhatsApp, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਈਮੇਲ ਜਾਂ ਅਣਜਾਣ ਵੈਬਸਾਈਟਾਂ 'ਤੇ ਮਿਲਦੇ ਹਨ ਅਤੇ ਦਿਖਣ ਵਿੱਚ ਬਿਲਕੁਲ ਸਧਾਰਨ ਜਾਂ ਆਕਰਸ਼ਕ ਲੱਗ ਸਕਦੇ ਹਨ। ਕਈ ਵਾਰ ਇਹ ਲਿੰਕ ਕਿਸੇ ਇਨਾਮ, ਡਿਸਕਾਊਂਟ, ਡਿਲੀਵਰੀ ਸਮੱਸਿਆ ਜਾਂ ਬੈਂਕ ਚੇਤਾਵਨੀ ਦੀ ਝੂਠੀ ਜਾਣਕਾਰੀ ਦੇ ਨਾਂ 'ਤੇ ਯੂਜ਼ਰ ਨੂੰ ਕਲਿੱਕ ਕਰਨ ਲਈ ਮਜਬੂਰ ਕਰਦੇ ਹਨ। ਜਦੋਂ ਕੋਈ ਵਿਅਕਤੀ ਅਜਿਹੇ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਦਾ ਹੈ, ਤਾਂ ਉਹ ਕਿਸੇ ਨਕਲੀ ਵੈਬਸਾਈਟ 'ਤੇ ਪਹੁੰਚ ਸਕਦਾ ਹੈ ਜਾਂ ਉਸਦੇ ਫੋਨ-ਕੰਪਿਊਟਰ ਵਿੱਚ ਮਾਲਵੇਅਰ, ਵਾਇਰਸ ਜਾਂ ਸਪਾਈਵੇਅਰ ਇੰਸਟਾਲ ਹੋ ਸਕਦਾ ਹੈ, ਜੋ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਨ, ਪਾਸਵਰਡ ਲੈਣ ਜਾਂ ਪੈਸਾ ਚੁਰਾਉਣ ਲਈ ਵਰਤਿਆ ਜਾਂਦਾ ਹੈ। ਇਸ ਕਰਕੇ, ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਜਾਂ ਸ਼ੱਕੀ ਲਿੰਕ 'ਤੇ ਕਦੇ ਵੀ ਕਲਿੱਕ ਨਹੀਂ ਕਰਨਾ ਚਾਹੀਦਾ, ਭਾਵੇਂ ਉਹ ਕਿੰਨਾ ਹੀ ਭਰੋਸੇਮੰਦ ਜਾਂ ਲੁਭਾਉਣ ਵਾਲਾ ਕਿਉਂ ਨਾ ਲੱਗੇ। ਹਮੇਸ਼ਾਂ ਭੇਜਣ ਵਾਲੇ ਦੀ ਪਛਾਣ ਦੀ ਜਾਂਚ ਕਰੋ, ਵੈਬਸਾਈਟ ਦਾ ਐਡਰੈੱਸ ਧਿਆਨ ਨਾਲ ਵੇਖੋ, ਅਧਿਕਾਰਤ ਐਪਸ ਦੀ ਵਰਤੋਂ ਕਰੋ ਅਤੇ ਜੇ ਕੋਈ ਸੰਦੇਹ ਹੋਵੇ ਤਾਂ ਲਿੰਕ ਨੂੰ ਪੂਰੀ ਤਰ੍ਹਾਂ ਨਜ਼ਰਅੰਦਾਜ਼ ਕਰੋ। ਸਾਵਧਾਨੀ ਹੀ ਡਿਜ਼ਿਟਲ ਸੁਰੱਖਿਆ ਦੀ ਸਭ ਤੋਂ ਵੱਡੀ ਕੁੰਜੀ ਹੈ।

6. ਵਿਦਿਆਰਥੀਆਂ ਵਿੱਚ ਆਨਲਾਈਨ ਗੇਮਾਂ ਖੇਡਣ ਦੀ ਆਦਤ ਅਤੇ ਇਸ ਸਬੰਧੀ ਸੁਝਾਅ

ਆਨਲਾਈਨ ਗੇਮਿੰਗ ਮਜ਼ੇਦਾਰ ਅਤੇ ਮਨੋਰੰਜਕ ਹੁੰਦੀ ਹੈ, ਪਰ ਇਸਦੇ ਨਾਲ ਕੁਝ ਸੁਰੱਖਿਆ ਖਤਰੇ ਵੀ ਜੁੜੇ ਹੋਏ ਹਨ ਜਿਨ੍ਹਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹਿਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਸਭ ਤੋਂ ਪਹਿਲਾਂ, ਗੇਮ ਖੇਡਦੇ ਸਮੇਂ ਕਦੇ ਵੀ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਨਾਮ, ਪਤਾ, ਫੋਨ ਨੰਬਰ, ਸਕੂਲ ਦਾ ਨਾਂ, ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤੇ ਕਿਸੇ ਨਾਲ ਸਾਂਝੇ ਨਾ ਕਰੋ, ਕਿਉਂਕਿ ਅਣਜਾਣ ਲੋਕ ਇਸ ਜਾਣਕਾਰੀ ਦਾ ਗ਼ਲਤ ਫਾਇਦਾ ਚੁੱਕ ਸਕਦੇ ਹਨ। ਬਹੁਤ ਸਾਰੀਆਂ ਗੇਮਾਂ ਵਿੱਚ ਚੈਟਿੰਗ ਫੀਚਰ ਹੁੰਦਾ ਹੈ, ਪਰ ਅਣਜਾਣ ਖਿਡਾਰੀਆਂ ਨਾਲ ਗੱਲਬਾਤ ਕਰਨਾ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹੁੰਦਾ ਕਿਉਂਕਿ ਉਹ ਠੱਗ, ਸਾਈਬਰ ਬੁਲੀ ਜਾਂ ਫਰਾਡ ਕਰਨ ਵਾਲੇ ਵੀ ਹੋ ਸਕਦੇ ਹਨ।



ਗੇਮਿੰਗ ਐਡਿਕਸ਼ਨ ਵੀ ਇੱਕ ਗੰਭੀਰ ਸਮੱਸਿਆ ਹੈ, ਇਸ ਲਈ ਖੇਡਣ ਲਈ ਸਮਾਂ ਨਿਰਧਾਰਿਤ ਕਰੋ, ਨਿਯਮਿਤ ਬ੍ਰੇਕ ਲਵੋ ਅਤੇ ਪੜ੍ਹਾਈ ਜਾਂ ਕੰਮ ਨੂੰ ਕਦੇ ਵੀ ਨੁਕਸਾਨ ਨਾ ਹੋਣ ਦਿਓ।

ਗੇਮਾਂ ਵਿੱਚ ਦਿੱਤੀਆਂ **In-app purchases** ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ। ਕਈ ਵਾਰ ਬੱਚੇ ਜਾਂ ਵੱਡੇ ਗੇਮ ਦੇ ਦਬਾਅ ਵਿੱਚ ਬਿਨਾਂ ਸੋਚੇ ਸਮਝੇ ਪੈਸੇ ਖਰਚ ਦਿੰਦੇ ਹਨ, ਇਸ ਲਈ ਪਾਸਵਰਡ ਜਾਂ ਫਿੰਗਰਪ੍ਰਿੰਟ ਲਾਕ ਜ਼ਰੂਰ ਲਗਾਓ। ਇਸਦੇ ਨਾਲ ਨਾਲ, ਹਮੇਸ਼ਾਂ

ਅਧਿਕਾਰਤ ਐਪ ਸਟੋਰ ਤੋਂ ਹੀ ਗੇਮਾਂ ਡਾਊਨਲੋਡ ਕਰੋ ਤਾਂ ਜੋ ਮਾਲਵੇਅਰ ਤੋਂ ਬਚਿਆ ਜਾ ਸਕੇ। ਕੁੱਲ ਮਿਲਾ ਕੇ, ਜੇ ਚੇਤਾਵਨੀ, ਸਾਵਧਾਨੀ ਅਤੇ ਸਹੀ ਡਿਜ਼ਿਟਲ ਆਦਤਾਂ ਅਪਣਾਈਆਂ ਜਾਣ, ਤਾਂ ਆਨਲਾਈਨ ਗੇਮਿੰਗ ਨੂੰ ਸੁਰੱਖਿਅਤ ਅਤੇ ਮਜ਼ੇਦਾਰ ਤਜਰਬਾ ਬਣਾਇਆ ਜਾ ਸਕਦਾ ਹੈ।

ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਚੈਟ ਨਾ ਕਰਨੀ

ਆਨਲਾਈਨ ਗੇਮਾਂ ਵਿੱਚ ਅਕਸਰ ਚੈਟ ਫੀਚਰ ਹੁੰਦਾ ਹੈ ਜਿਸ ਨਾਲ ਖਿਡਾਰੀ ਆਪਸ ਵਿੱਚ ਗੱਲਬਾਤ ਕਰ ਸਕਦੇ ਹਨ, ਪਰ ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਚੈਟ ਕਰਨਾ ਖਤਰੇ ਨਾਲ ਭਰਿਆ ਹੋ ਸਕਦਾ ਹੈ। ਬਹੁਤ ਵਾਰ ਨਕਲੀ ਪ੍ਰੋਫਾਈਲ, ਦੁਸ਼ਟ ਇਰਾਦੇ ਵਾਲੇ ਜਾਂ ਸਾਈਬਰ ਬੁਲੀ ਅਜਿਹੀਆਂ ਗੇਮਾਂ ਵਿੱਚ ਲੋਕਾਂ ਨੂੰ ਪਟਾਉਣ, ਡਰਾਉਣ ਜਾਂ ਉਨ੍ਹਾਂ ਤੋਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਲੈਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦੇ ਹਨ। ਉਹ ਨਾਮ, ਪਤਾ, ਉਮਰ, ਫੋਨ ਨੰਬਰ, ਤਸਵੀਰਾਂ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤਿਆਂ ਦੀ ਮੰਗ ਕਰ ਸਕਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਗੋਪਨੀਯਤਾ ਅਤੇ ਸੁਰੱਖਿਆ ਨੂੰ ਖਤਰਾ ਬਣ ਜਾਂਦਾ ਹੈ। ਕਈ ਠੱਗ ਗੇਮ ਦੇ ਅੰਦਰ ਦੇਸਤੀ ਦਾ ਨਾਟਕ ਕਰਕੇ ਬੱਚਿਆਂ ਜਾਂ ਨੌਜਵਾਨਾਂ ਨੂੰ Fraud Links ਜਾਂ ਨਕਲੀ ਆਫਰ ਭੇਜਦੇ ਹਨ, ਜੋ ਬਹੁਤ ਹੀ ਖਤਰਨਾਕ ਹੋ ਸਕਦੇ ਹਨ। ਇਸ ਲਈ ਹਮੇਸ਼ਾਂ ਚੇਤਾਵਨੀ ਰੱਖੋ ਕਿ ਆਨਲਾਈਨ ਗੇਮ ਵਿੱਚ ਕਦੇ ਵੀ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਕਿਸੇ ਨੂੰ ਨਾ ਦਿਓ, ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਚੈਟ ਨਾ ਕਰੋ, ਅਤੇ ਜੇ ਕੋਈ ਸ਼ੱਕੀ ਵਿਅਕਤੀ ਮੇਸੇਜ ਕਰੇ ਤਾਂ ਉਸਨੂੰ ਤੁਰੰਤ ਬਲੋਕ ਕਰ ਦਿਓ।

ਗੇਮਿੰਗ ਐਡਿਕਸ਼ਨ ਤੋਂ ਸਾਵਧਾਨੀ

ਆਨਲਾਈਨ ਗੇਮਿੰਗ ਮਜ਼ੇਦਾਰ ਹੁੰਦੀ ਹੈ, ਪਰ ਜੇ ਇਹ ਆਦਤ ਬਣ ਜਾਵੇ ਤਾਂ ਇਹ ਮਨੋਵਿਗਿਆਨਕ, ਸਿਹਤਮੰਦ ਅਤੇ ਸਿੱਖਿਆ/ਰੋਜ਼ਾਨਾ ਜੀਵਨ ਤੇ ਗੰਭੀਰ ਪ੍ਰਭਾਵ ਪਾ ਸਕਦੀ ਹੈ। ਗੇਮਿੰਗ ਐਡਿਕਸ਼ਨ ਨਾਲ ਵਿਅਕਤੀ ਦਾ ਧਿਆਨ ਪੜ੍ਹਾਈ ਜਾਂ ਕੰਮ ਤੋਂ ਹਟ ਜਾਂਦਾ ਹੈ, ਨੀਂਦ ਘੱਟ ਹੋ ਜਾਂਦੀ ਹੈ, ਖਾਣ-ਪੀਣ ਦੀ ਰੁਟੀਨ ਵਿਗੜਦੀ ਹੈ ਅਤੇ ਮਨ 'ਚ ਬੇਚੈਨੀ, ਗੁੱਸਾ ਅਤੇ ਚਿੜਚਿੜਾਪਣ ਵਧ ਜਾਂਦਾ ਹੈ। ਕਈ ਲੋਕ ਰਾਤਾਂ ਜਾਗ ਕੇ ਗੇਮ ਖੇਡਦੇ ਹਨ ਜਿਸ ਨਾਲ ਸਿਹਤ ਖਰਾਬ ਹੁੰਦੀ ਹੈ ਅਤੇ ਦਿਮਾਗ 'ਤੇ ਬੁਰਾ ਅਸਰ ਪੈਂਦਾ ਹੈ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਗੇਮਾਂ ਵਿੱਚ ਲੈਵਲ ਅੱਪ ਕਰਨ ਦੀ ਲਾਲਸਾ, ਇਨਾਮ ਜਿੱਤਣ ਦੀ ਭਾਵਨਾ, ਅਤੇ ਦੇਸਤਾਂ ਨਾਲ ਮੁਕਾਬਲੇ ਦਾ ਦਬਾਅ ਐਡਿਕਸ਼ਨ ਨੂੰ ਹੋਰ ਵਧਾ ਸਕਦਾ ਹੈ। ਗੇਮਿੰਗ ਐਡਿਕਸ਼ਨ ਤੋਂ ਬਚਣ ਦਾ ਸਭ ਤੋਂ ਵਧੀਆ ਤਰੀਕਾ ਹੈ **ਸਮਾਂ ਸੀਮਾ ਨਿਰਧਾਰਿਤ ਕਰਨਾ**, ਸਕਰੀਨ ਤੋਂ ਨਿਯਮਿਤ ਬ੍ਰੇਕ ਲੈਣਾ, ਘਰੇਲੂ ਅਤੇ ਬਾਹਰੀ ਗਤਿਵਿਧੀਆਂ

ਵਿੱਚ ਸ਼ਾਮਲ ਹੋਣਾ, ਅਤੇ ਆਪਣੇ ਆਪ ਨੂੰ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਯਾਦ ਦਿਵਾਉਣਾ ਕਿ ਗੇਮ ਸਿਰਫ਼ ਮਨੋਰੰਜਨ ਲਈ ਹੈ। ਜੇ ਕੋਈ ਵਿਅਕਤੀ ਖੁਦ ਨੂੰ ਰੋਕ ਨਹੀਂ ਸਕਦਾ, ਤਾਂ ਮਾਪਿਆਂ, ਅਧਿਆਪਕਾਂ ਜਾਂ ਕਿਸੇ ਮਾਹਰ ਨਾਲ ਗੱਲ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ।

In-app purchases ਤੋਂ ਬਚਾਅ

ਬਹੁਤ ਸਾਰੀਆਂ ਆਨਲਾਈਨ ਗੇਮਾਂ ਵਿੱਚ **In-app purchases** ਹੁੰਦੀਆਂ ਹਨ, ਜਿਵੇਂ ਕਿ ਕੋਇਨ, ਜੈਮ, ਸਕਿਨ, ਸ਼ਸਤ੍ਰ, ਲੈਵਲ ਬੁਸਟ ਜਾਂ ਹੋਰ ਆਈਟਮ ਖਰੀਦਣ ਲਈ ਪੈਸੇ ਲੱਗਦੇ ਹਨ। ਬੱਚੇ ਅਤੇ ਕਈ ਵਾਰ ਬਾਲਗ ਵੀ ਗੇਮ ਵਿੱਚ ਪ੍ਰਗਤੀ ਕਰਨ ਜਾਂ ਦੇਸਤਾਂ ਨੂੰ ਪ੍ਰਭਾਵਿਤ ਕਰਨ ਲਈ ਇਹ ਚੀਜ਼ਾਂ ਖਰੀਦਣ ਦੀ ਸੋਚ ਲੈਂਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਕਈ ਵਾਰ ਬਿਨਾਂ ਲੋੜੇ ਪੈਸੇ ਖਰਚ ਹੋ ਜਾਂਦੇ ਹਨ। ਕੁਝ ਗੇਮਾਂ ਲੁਭਾਉਣ ਵਾਲੇ ਤਰੀਕਿਆਂ ਨਾਲ ਖਿਡਾਰੀ ਨੂੰ ਖਰੀਦਦਾਰੀ ਕਰਨ ਲਈ ਉਕਸਾਉਂਦੀਆਂ ਹਨ, ਜਿਵੇਂ “Limited Offer”, “One-time Deal”, ਜਾਂ “Only 5 minutes left”. ਕਈ ਵਾਰ ਬਿਨਾਂ ਜਾਣਕਾਰੀ ਦੇ ਬੱਚੇ ਮੋਬਾਈਲ ਵਿੱਚ ਜੁੜੇ ਕਾਰਡ ਜਾਂ UPI ਤੋਂ ਖਰੀਦਦਾਰੀ ਕਰ ਦਿੰਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਵੱਡਾ ਆਰਥਿਕ ਨੁਕਸਾਨ ਵੀ ਹੋ ਸਕਦਾ ਹੈ। ਇਸ ਲਈ In-app purchases ਤੋਂ ਬਚਣ ਲਈ ਮਾਪੇ **Parental Controls** ਲਗਾ ਸਕਦੇ ਹਨ, ਪਾਸਵਰਡ ਜਾਂ ਬਾਯੋਮੈਟ੍ਰਿਕ ਲਾਕ ਲਗਾਉਣ ਚਾਹੀਦੇ ਹਨ ਅਤੇ ਬੱਚਿਆਂ ਨੂੰ ਇਸ ਬਾਰੇ ਸਿੱਖਿਆ ਦੇਣੀ ਜ਼ਰੂਰੀ ਹੈ। ਗੇਮ ਖੇਡਣ ਵੇਲੇ ਹਮੇਸ਼ਾਂ ਇਹ ਸੁਨਿਸ਼ਚਿਤ ਕਰੋ ਕਿ ਕੋਈ ਅਣਚਾਹੀ ਖਰੀਦਦਾਰੀ ਨਾ ਹੋਵੇ ਅਤੇ ਪੈਸੇ ਸਿਰਫ਼ ਜ਼ਰੂਰਤ ਹੋਣ 'ਤੇ ਅਤੇ ਸੋਚ-ਵਿਚਾਰ ਕਰਕੇ ਹੀ ਖਰਚੇ ਜਾਣ।

7. ਡਿਜਿਟਲ ਐਟਿਕੇਟ ਦਾ ਮਤਲਬ ਅਤੇ ਇਸ ਦੀ ਜ਼ਰੂਰਤ

ਡਿਜਿਟਲ ਐਟਿਕੇਟ ਦਾ ਮਤਲਬ ਹੈ ਇੰਟਰਨੈੱਟ ਅਤੇ ਡਿਜਿਟਲ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ ਜ਼ਿੰਮੇਵਾਰ, ਸਤਿਕਾਰੀ ਅਤੇ ਸੋਚ-ਵਿਚਾਰ ਨਾਲ ਵਰਤਾਓ ਕਰਨਾ। ਜਿਵੇਂ ਅਸੀਂ ਹਕੀਕਤ ਵਿੱਚ ਸ਼ਿਸ਼ਟਾਚਾਰ ਦੀ ਪਾਲਣਾ ਕਰਦੇ ਹਾਂ, ਉਸੇ ਤਰ੍ਹਾਂ ਆਨਲਾਈਨ ਸੰਚਾਰ ਵਿੱਚ ਵੀ ਨਿਯਮਾਂ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ। ਇਸ ਵਿੱਚ ਸਭ ਤੋਂ ਪਹਿਲਾਂ **ਸਹੀ ਭਾਸ਼ਾ ਅਤੇ ਤਹਿਜੀਬ** ਨਾਲ ਗੱਲਬਾਤ ਕਰਨੀ ਸ਼ਾਮਲ ਹੈ। ਕਿਸੇ 'ਤੇ ਗੁੱਸਾ ਕਰਨਾ, ਬੁਰੇ ਕਮੈਂਟ ਕਰਨਾ ਜਾਂ ਕਿਸੇ ਦੀ ਬੇਇਜ਼ਤੀ ਕਰਨਾ ਡਿਜਿਟਲ ਐਟਿਕੇਟ ਦੇ ਖਿਲਾਫ਼ ਹੈ। ਆਨਲਾਈਨ ਗੱਲਬਾਤ ਦੌਰਾਨ ਹੋਰਨਾਂ ਦੀ ਨਿੱਜਤਾ ਦੀ ਰੱਖਿਆ ਕਰਨਾ ਵੀ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ—ਕਿਸੇ ਦੀ ਤਸਵੀਰ, ਵੀਡੀਓ ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਬਿਨਾਂ ਮਨਜ਼ੂਰੀ ਦੇ ਸਾਂਝੀ ਨਹੀਂ ਕਰਨੀ ਚਾਹੀਦੀ।



ਡਿਜਿਟਲ ਐਟਿਕੇਟ ਵਿੱਚ **ਫੇਕ ਨਿਊਜ਼** ਜਾਂ **ਅਫਵਾਹਾਂ** ਨੂੰ ਫੈਲਾਉਣ ਤੋਂ ਬਚਣਾ ਵੀ ਸ਼ਾਮਲ ਹੈ, ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਹੋਰ ਲੋਕਾਂ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚ ਸਕਦਾ ਹੈ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਗਰੁੱਪਾਂ ਅਤੇ ਕਲਾਸਰੂਮਾਂ ਵਿੱਚ ਆਨਲਾਈਨ ਪ੍ਰੈਫੈਸ਼ਨਲ ਵਿਹਾਰ ਰੱਖਣਾ, ਅਧਿਆਪਕਾਂ ਅਤੇ ਸਾਥੀਆਂ ਦਾ ਸਤਿਕਾਰ ਕਰਨਾ ਵੀ ਲਾਜ਼ਮੀ ਹੈ। ਜਦੋਂ ਵੀ ਕੋਈ ਚੈਟ, ਟਿੱਪਣੀ ਜਾਂ ਪੋਸਟ ਕਰੇ, ਪਹਿਲਾਂ ਸੋਚੋ ਕਿ ਇਸਦਾ ਹੋਰਨਾਂ 'ਤੇ ਕੀ ਅਸਰ ਪਵੇਗਾ। ਡਿਜਿਟਲ ਐਟਿਕੇਟ ਇਹ ਵੀ ਸਿਖਾਉਂਦਾ ਹੈ ਕਿ ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਵਰਤੋ, ਅਣਜਾਣ ਲਿੰਕਾਂ ਤੋਂ ਬਚੋ ਅਤੇ ਹੋਰਨਾਂ ਨੂੰ ਵੀ ਸੁਰੱਖਿਆ ਬਾਰੇ ਸਚੇਤ ਕਰੋ।

ਡਿਜਿਟਲ ਐਟਿਕੇਟ ਦਾ ਮਕਸਦ ਆਨਲਾਈਨ ਦੁਨੀਆ ਨੂੰ ਸਤਿਕਾਰ, ਸੁਰੱਖਿਆ, ਸਹਿਯੋਗ ਅਤੇ ਸਕਾਰਾਤਮਕਤਾ ਨਾਲ ਭਰਪੂਰ ਬਣਾਉਣਾ ਹੈ, ਤਾਂ ਜੋ ਹਰ ਉਪਭੋਗਤਾ ਇੱਕ ਸੁਰੱਖਿਅਤ ਅਤੇ ਸੁੰਤਲਿਤ ਡਿਜਿਟਲ ਅਨੁਭਵ ਦਾ ਆਨੰਦ ਲੈ ਸਕੇ।

ਆਨਲਾਈਨ ਵਿਹਾਰ ਦੇ ਨਿਯਮ

ਆਨਲਾਈਨ ਵਿਹਾਰ ਦੇ ਨਿਯਮ, ਜਿਨ੍ਹਾਂ ਨੂੰ ਕਈ ਵਾਰੀ **ਡਿਜਿਟਲ ਮੈਨਰਜ਼** ਵੀ ਕਹਿੰਦੇ ਹਨ, ਇੰਟਰਨੈੱਟ 'ਤੇ ਸਹੀ, ਸੁਰੱਖਿਅਤ ਅਤੇ ਨੈਤਿਕ ਵਰਤੋਂ ਨੂੰ ਯਕੀਨੀ ਬਣਾਉਂਦੇ ਹਨ।

1. **ਸਹੀ ਭਾਸ਼ਾ ਅਤੇ ਤਹਿਜ਼ੀਬ ਨਾਲ ਸੰਚਾਰ ਕਰਨਾ** ਜ਼ਰੂਰੀ ਹੈ। ਚੈਟ, ਕਮੈਂਟ ਜਾਂ ਈਮੇਲ ਵਿੱਚ ਗੁੱਸਾ, ਬਦਸਲੂਕੀ ਜਾਂ ਗੰਦੇ ਸ਼ਬਦ ਵਰਤਣ ਤੋਂ ਬਚੋ।
2. **ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰੋ**, ਜਿਵੇਂ ਨਾਮ, ਪਤਾ, ਫੋਨ ਨੰਬਰ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤੇ, ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਸੁਰੱਖਿਆ ਖਤਰੇ ਵਿੱਚ ਆ ਸਕਦੀ ਹੈ।
3. **ਆਨਲਾਈਨ ਨਕਲੀ ਜਾਣਕਾਰੀ ਜਾਂ ਫੇਕ ਨਿਊਜ਼ ਨੂੰ ਨਾ ਫੈਲਾਓ**, ਅਤੇ ਹਮੇਸ਼ਾਂ ਜਾਣਕਾਰੀ ਦੇ ਸਹੀ ਸਰੋਤ ਦੀ ਜਾਂਚ ਕਰੋ।
4. **ਸੋਸ਼ਲ ਮੀਡੀਆ ਤੇ ਹੋਰਨਾਂ ਦੀ ਇੱਜ਼ਤ ਕਰੋ**; ਕਿਸੇ ਦੀ ਤਸਵੀਰ, ਵੀਡੀਓ ਜਾਂ ਪੋਸਟ ਬਿਨਾਂ ਮਨਜ਼ੂਰੀ ਦੇ ਸਾਂਝੀ ਨਾ ਕਰੋ।
5. **ਆਨਲਾਈਨ ਟ੍ਰੋਲਿੰਗ, ਬੁਲਿੰਗ ਜਾਂ ਡਰਾਉਣ ਵਾਲੇ ਸੁਨੇਹਿਆਂ ਤੋਂ ਬਚੋ**, ਅਤੇ ਜੇ ਕੋਈ ਸ਼ੱਕੀ ਵਿਅਕਤੀ ਸੰਪਰਕ ਕਰੇ, ਤਾਂ ਉਸਨੂੰ ਬਲੈਕ ਕਰੋ।

ਆਨਲਾਈਨ ਵਿਹਾਰ ਦੇ ਨਿਯਮ ਇਹ ਵੀ ਸਿਖਾਉਂਦੇ ਹਨ ਕਿ ਪਾਸਵਰਡ ਸੁਰੱਖਿਅਤ ਰੱਖੋ, ਅਣਜਾਣ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ ਅਤੇ ਡਿਜਿਟਲ ਪਲੇਟਫਾਰਮਾਂ ਨੂੰ ਚੰਗੇ ਇਰਾਦੇ ਨਾਲ ਵਰਤੋਂ। ਜੇ ਇਹ ਨਿਯਮ ਅਪਣਾਏ ਜਾਣ, ਤਾਂ ਆਨਲਾਈਨ ਦੁਨੀਆ ਸੁਰੱਖਿਅਤ, ਮਿੱਠਾ ਅਤੇ ਸਹਿਯੋਗੀ ਬਣਾਈ ਜਾ ਸਕਦੀ ਹੈ।

ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ

ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਦਾ ਮਤਲਬ ਹੈ ਇੰਟਰਨੈੱਟ ਅਤੇ ਡਿਜ਼ਿਟਲ ਪਲੇਟਫਾਰਮਾਂ ਨੂੰ ਸੱਚਾਈ, ਇਮਾਨਦਾਰੀ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਵਰਤਣਾ।

1. **ਕਾਪੀਰਾਈਟ ਅਤੇ ਬੌਧਿਕ ਸੰਪਤੀ ਦੀ ਪਾਲਣਾ** ਕਰਨੀ ਸ਼ਾਮਲ ਹੈ। ਕਿਸੇ ਹੋਰ ਦੀ ਲਿਖਤ, ਵੀਡੀਓ, ਗੀਤ ਜਾਂ ਸਾਫਟਵੇਅਰ ਬਿਨਾਂ ਮਨਜ਼ੂਰੀ ਵਰਤਣਾ ਗਲਤ ਹੈ ਅਤੇ ਇਸਨੂੰ ਕਾਨੂੰਨੀ ਤੌਰ 'ਤੇ ਅਪਰਾਧ ਮੰਨਿਆ ਜਾਂਦਾ ਹੈ।
2. **ਫੇਕ ਨਿਊਜ਼ ਜਾਂ ਗਲਤ ਜਾਣਕਾਰੀ ਨਾ ਫੈਲਾਉਣਾ** ਵੀ ਨੈਤਿਕ ਵਰਤੋਂ ਦਾ ਹਿੱਸਾ ਹੈ, ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਹੋਰਨਾਂ ਨੂੰ ਨੁਕਸਾਨ ਹੋ ਸਕਦਾ ਹੈ।
3. **ਆਨਲਾਈਨ ਲੈਣ-ਦੇਣ ਅਤੇ ਖਰੀਦਦਾਰੀ ਸੁਰੱਖਿਅਤ ਅਤੇ ਇਮਾਨਦਾਰੀ ਨਾਲ** ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। ਕਿਸੇ ਨੂੰ ਠੱਗਣਾ, Fraud Links 'ਤੇ ਭਰੋਸਾ ਕਰਨਾ ਜਾਂ ਬਿਨਾਂ ਇਜਾਜ਼ਤ ਪੈਸੇ ਕੱਢਣਾ ਗਲਤ ਹੈ।
4. **ਆਨਲਾਈਨ ਵਰਤੋਂ ਦੌਰਾਨ ਹੋਰਨਾਂ ਦੀ ਇੱਜ਼ਤ ਅਤੇ ਸੁਰੱਖਿਆ ਦਾ ਧਿਆਨ ਰੱਖਣਾ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਕਿਸੇ ਨੂੰ ਹੈਰਾਨ ਕਰਨਾ, ਬੁਲੰਗ ਕਰਨਾ ਜਾਂ ਅਣਜਾਣ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਲਈ ਉਕਸਾਉਣਾ ਨੈਤਿਕ ਨਹੀਂ ਹੈ।

ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਨਾਲ ਇੰਟਰਨੈੱਟ ਇੱਕ ਸੁਰੱਖਿਅਤ, ਸ਼ਿਸ਼ਟ ਅਤੇ ਸਹਿਯੋਗੀ ਮਾਹੌਲ ਬਣਦਾ ਹੈ, ਜਿਸ ਵਿੱਚ ਹਰ ਉਪਭੋਗਤਾ ਆਨੰਦ ਅਤੇ ਸੁਰੱਖਿਆ ਨਾਲ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਦਾ ਲੁਤਫ਼ ਉਠਾ ਸਕਦਾ ਹੈ। ਇਹ ਸਿਰਫ਼ ਨੈਤਿਕ ਨਹੀਂ, ਬਲਕਿ ਸੁਰੱਖਿਅਤ ਡਿਜ਼ਿਟਲ ਜੀਵਨ ਲਈ ਵੀ ਜ਼ਰੂਰੀ ਹੈ।

ਹੋਰਨਾਂ ਦੀ ਇੱਜ਼ਤ ਅਤੇ ਸੁਰੱਖਿਆ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਹੋਰਨਾਂ ਦੀ ਇੱਜ਼ਤ ਅਤੇ ਸੁਰੱਖਿਆ ਬਣਾਈ ਰੱਖਣਾ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਇਹ ਡਿਜ਼ਿਟਲ ਐਟਿਕੇਟ ਅਤੇ ਨੈਤਿਕ ਵਰਤੋਂ ਦਾ ਅਹੱਸਭਾਗ ਹੈ।

1. ਕਿਸੇ ਦੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਨਾਮ, ਪਤਾ, ਫੋਨ ਨੰਬਰ, ਤਸਵੀਰ ਜਾਂ ਵੀਡੀਓ ਬਿਨਾਂ ਉਸਦੀ ਮਨਜ਼ੂਰੀ ਦੇ ਸਾਂਝੀ ਨਾ ਕਰੋ। ਇਸ ਨਾਲ ਹੋਰਨਾਂ ਦੀ ਗੋਪਨੀਯਤਾ ਅਤੇ ਸੁਰੱਖਿਆ ਨੂੰ ਖਤਰਾ ਪਹੁੰਚਦਾ ਹੈ।

2. ਆਨਲਾਈਨ ਚੈਟ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਫੋਰਨਮ ਜਾਂ ਗੇਮਿੰਗ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ ਕਿਸੇ ਨਾਲ ਬੁਲੰਗ, ਟ੍ਰੋਲਿੰਗ ਜਾਂ ਗੰਦੇ ਸੁਨੇਹੇ ਨਾ ਭੇਜੋ। ਇਹ ਕਾਰਵਾਈ ਹੋਰਨਾਂ ਦੀ ਭਾਵਨਾਵਾਂ ਨੂੰ ਠੇਸ ਪਹੁੰਚਾ ਸਕਦੀ ਹੈ ਅਤੇ ਆਨਲਾਈਨ ਮਾਹੌਲ ਨੂੰ ਨਿਰਵਿਘਨ ਬਣਾਉਂਦੀ ਹੈ।
3. ਹਰ ਕਿਸੇ ਦੇ ਵਿਚਾਰਾਂ ਅਤੇ ਰਾਏ ਦੀ ਇੱਜ਼ਤ ਕਰੋ। ਵੱਖ-ਵੱਖ ਵਿਚਾਰ ਹੋ ਸਕਦੇ ਹਨ, ਪਰ ਇਹ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਸਹਿਮਤ ਹੋਣ ਜਾਂ ਨਾ ਹੋਣ ਦੇ ਬਾਵਜੂਦ ਗੱਲਬਾਤ ਸ਼ਾਂਤ ਅਤੇ ਸੰਵਿਧਾਨਕ ਰਹੇ।
4. ਅਣਜਾਣ ਲਿੰਕ, ਨਕਲੀ ਆਫਰ ਜਾਂ ਧੋਖੇਬਾਜ਼ੀ ਵਾਲੇ ਸੰਦੇਸ਼ਾਂ ਨਾਲ ਹੋਰਨਾਂ ਨੂੰ ਬਚਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ। ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਵਰਤੋ ਅਤੇ ਆਪਣੇ ਅਤੇ ਹੋਰਨਾਂ ਦੇ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਸਚੇਤ ਰਹੋ।

ਸੰਖੇਪ ਵਿੱਚ, ਹੋਰਨਾਂ ਦੀ ਇੱਜ਼ਤ ਅਤੇ ਸੁਰੱਖਿਆ ਨੂੰ ਯਕੀਨੀ ਬਣਾਉਣ ਨਾਲ ਆਨਲਾਈਨ ਦੁਨੀਆ ਸੁਰੱਖਿਅਤ, ਸਿਸ਼ਟ ਅਤੇ ਸਹਿਯੋਗੀ ਬਣਦੀ ਹੈ। ਇਹ ਹਰ ਉਪਭੋਗਤਾ ਲਈ ਆਨੰਦ ਅਤੇ ਸੁਰੱਖਿਆ ਦੋਹਾਂ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ।

8. ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਸਬੰਧੀ ਜ਼ਰੂਰੀ ਸੁਝਾਅ

ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਅੱਜ ਦੇ ਡਿਜਿਟਲ ਯੁੱਗ ਵਿੱਚ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਵਿੱਚ ਉਹ ਸਾਰਾ ਡਾਟਾ ਸ਼ਾਮਲ ਹੈ ਜੋ ਕਿਸੇ ਵਿਅਕਤੀ ਨੂੰ ਪਛਾਣਨ ਲਈ ਵਰਤਿਆ ਜਾ ਸਕਦਾ ਹੈ, ਜਿਵੇਂ ਨਾਮ, ਪਤਾ, ਫੋਨ ਨੰਬਰ, ਪਾਸਵਰਡ, ਬੈਂਕ ਖਾਤਾ ਨੰਬਰ, ਆਧਾਰ ਨੰਬਰ, ਇਮੇਲ ਐਡਰੈੱਸ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤੇ। ਜੇ ਇਹ ਜਾਣਕਾਰੀ ਗਲਤ ਹੱਥਾਂ ਵਿੱਚ ਚਲੀ ਜਾਂਦੀ ਹੈ, ਤਾਂ ਇਸ ਨਾਲ ਪਛਾਣ ਚੋਰੀ, ਫਰਾਡ, ਹੈਕਿੰਗ ਅਤੇ ਹੋਰ ਸਾਈਬਰ ਜੁਰਮ ਹੋ ਸਕਦੇ ਹਨ।



ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਲਈ ਕੁਝ ਮੁੱਖ ਤਰੀਕੇ ਹਨ:

1. ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਅਤੇ ਟੂ-ਫੈਕਟਰ ਆਥੈਂਟੀਕੇਸ਼ਨ (2FA) ਵਰਤਣਾ ਚਾਹੀਦਾ ਹੈ।
2. ਅਣਜਾਣ ਲਿੰਕ, ਈਮੇਲਾਂ ਅਤੇ ਐਟੈਚਮੈਂਟਾਂ ਤੋਂ ਬਚਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।
3. ਆਪਣਾ ਡਾਟਾ ਹਮੇਸ਼ਾਂ ਸੁਰੱਖਿਅਤ ਸਰਵਰਾਂ ਅਤੇ ਐਪਸ 'ਤੇ ਹੀ ਸਾਂਝਾ ਕਰੋ ਅਤੇ ਅਣਜਾਣ ਐਪਸ ਜਾਂ ਵੈਬਸਾਈਟਾਂ ਨੂੰ ਐਕਸੈੱਸ ਨਾ ਦੇਵੋ।

4. ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਪ੍ਰਚਾਰ ਨਾ ਕਰੋ; ਆਪਣੇ ਲੋਕਾਂ ਅਤੇ ਦੇਸ਼ਾਂ ਨਾਲ ਵੀ ਸਾਵਧਾਨ ਰਹੋ ਕਿ ਉਹ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਗਲਤ ਹੱਥਾਂ ਵਿੱਚ ਨਾ ਪਹੁੰਚਣ ਦਿਉ।

ਹੋਰ ਸਾਵਧਾਨੀਆਂ ਵਿੱਚ ਪਾਸਵਰਡ ਰੈਗੂਲਰ ਰੀਸੈੱਟ ਕਰਨਾ, ਪਬਲਿਕ Wi-Fi ਤੋਂ ਬਚਣਾ, ਅਤੇ ਮੋਬਾਈਲ ਅਤੇ ਕੰਪਿਊਟਰ ਵਿੱਚ ਐਂਟੀਵਾਇਰਸ/ਸੁਰੱਖਿਆ ਐਪਸ ਵਰਤਣਾ ਸ਼ਾਮਲ ਹੈ। ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ ਨਾ ਸਿਰਫ਼ ਖੁਦ ਨੂੰ ਬਚਾਉਂਦੀ ਹੈ, ਸਗੋਂ ਹੋਰਨਾਂ ਦੀ ਵੀ ਸੁਰੱਖਿਆ ਯਕੀਨੀ ਬਣਾਉਂਦੀ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ, ਸਾਵਧਾਨ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂ ਨਾਲ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਸੁਰੱਖਿਅਤ ਅਤੇ ਵਿਸ਼ਵਾਸਯੋਗ ਬਣਾਈ ਜਾ ਸਕਦੀ ਹੈ।

ਕਿਹੜੀ ਜਾਣਕਾਰੀ ਕਦੇ ਵੀ ਸਾਂਝੀ ਨਹੀਂ ਕਰਨੀ

ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਆ ਲਈ ਇਹ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਅਸੀਂ ਕੁਝ ਨਿੱਜੀ ਜਾਣਕਾਰੀਆਂ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝੀਆਂ ਨਾ ਕਰੀਏ।

1. ਪਾਸਵਰਡ ਅਤੇ ਪਿਨ ਨੰਬਰ ਬਿਲਕੁਲ ਗੁਪਤ ਰੱਖਣੇ ਚਾਹੀਦੇ ਹਨ। ਇਹ ਤੁਹਾਡੇ ਬੈਂਕ ਖਾਤੇ, ਡਿਜ਼ਿਟਲ ਵਾਲੇਟ, ਈਮੇਲ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹਨ।
2. ਬੈਂਕ ਖਾਤਾ ਨੰਬਰ, ਕਾਰਡ ਨੰਬਰ, CVV ਕੋਡ ਅਤੇ UPI ਪਿੰਨ ਕਿਸੇ ਨਾਲ ਵੀ ਸਾਂਝੇ ਨਾ ਕਰੋ, ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਪੈਸਾ ਚੋਰੀ ਹੋ ਸਕਦਾ ਹੈ।
3. ਨਿੱਜੀ ਪਤਾ, ਫੋਨ ਨੰਬਰ ਅਤੇ ਆਧਾਰ ਜਾਂ ਪੈਨ ਨੰਬਰ ਬਿਨਾਂ ਜ਼ਰੂਰਤ ਦੇ ਕਿਸੇ ਨਾਲ ਸਾਂਝੇ ਨਾ ਕਰੋ। ਇਹ ਜਾਣਕਾਰੀ ਗਲਤ ਹੱਥਾਂ ਵਿੱਚ ਚਲੀ ਜਾਂਦੀ ਹੈ ਤਾਂ ਤੁਹਾਡੀ ਪਛਾਣ ਚੋਰੀ ਅਤੇ ਸੁਰੱਖਿਆ ਨੂੰ ਖਤਰਾ ਹੋ ਸਕਦਾ ਹੈ।
4. ਤਸਵੀਰਾਂ, ਵੀਡੀਓ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤੇ ਦੀ ਜਾਣਕਾਰੀ ਬਿਨਾਂ ਮਨਜ਼ੂਰੀ ਦੇ ਸਾਂਝੀ ਨਾ ਕਰੋ, ਕਿਉਂਕਿ ਇਹ ਡਿਜ਼ਿਟਲ ਫਰਾਡ ਅਤੇ ਸਾਇਬਰ ਬੁਲਿੰਗ ਦਾ ਕਾਰਨ ਬਣ ਸਕਦੀ ਹੈ।

ਹਮੇਸ਼ਾਂ ਯਾਦ ਰੱਖੋ ਕਿ ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ, ਈਮੇਲ, SMS ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਮੈਸੇਜ 'ਤੇ ਆ ਕੇ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਮੰਗੇ ਤਾਂ ਇਹ ਧੋਖਾ ਹੋ ਸਕਦਾ ਹੈ। ਸੁਰੱਖਿਆ ਅਤੇ ਨਿੱਜਤਾ ਯਕੀਨੀ ਬਣਾਉਣ ਲਈ ਸਿਰਫ਼ ਭਰੋਸੇਮੰਦ ਸਰੋਤਾਂ ਨਾਲ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰੋ। ਇਹ ਸਾਵਧਾਨੀ ਤੁਹਾਨੂੰ ਅਤੇ ਹੋਰਨਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਂਦੀ ਹੈ।

Aadhaar, School ID, OTP, Bank info ਆਦਿ ਦੀ ਸੁਰੱਖਿਆ

Aadhaar, School ID, OTP ਅਤੇ Bank ਜਾਣਕਾਰੀ ਬਹੁਤ ਸੰਵੇਦਨਸ਼ੀਲ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਹੁੰਦੀ ਹੈ, ਜਿਸਦੀ ਸੁਰੱਖਿਆ ਕਰਨੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਕਿਉਂਕਿ ਇਹ ਗਲਤ ਹੱਥਾਂ ਵਿੱਚ ਜਾਣ 'ਤੇ ਵੱਡੇ ਨੁਕਸਾਨ ਦਾ ਕਾਰਨ ਬਣ ਸਕਦੀ ਹੈ। Aadhaar ਨੰਬਰ ਤੁਹਾਡੇ ਬਾਰੇ ਕਈ ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀਆਂ ਨਾਲ ਜੁੜਿਆ ਹੁੰਦਾ ਹੈ, ਇਸ ਲਈ ਇਸਨੂੰ ਕਦੇ ਵੀ ਅਣਜਾਣ ਵੈਬਸਾਈਟਾਂ, ਠੱਗੀ ਵਾਲੇ ਫਾਰਮਾਂ ਜਾਂ ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ। School ID ਵੀ ਬੱਚਿਆਂ ਦੀ ਪਛਾਣ ਅਤੇ ਸੁਰੱਖਿਆ ਨਾਲ ਜੁੜੀ ਹੁੰਦੀ ਹੈ, ਇਸ ਲਈ ਇਸਨੂੰ ਬਿਨਾਂ ਲੋੜ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਕਰਨਾ ਖਤਰਾ ਪੈਦਾ ਕਰ ਸਕਦਾ ਹੈ।

OTP (One-Time Password) ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਸੁਰੱਖਿਆ ਕੋਡ ਹੁੰਦਾ ਹੈ। ਬੈਂਕ, UPI ਜਾਂ ਕਿਸੇ ਵੀ ਡਿਜ਼ੀਟਲ ਸਰਵਿਸ ਲਈ ਆਉਣ ਵਾਲਾ OTP ਕਿਸੇ ਵੀ ਵਿਅਕਤੀ ਇਥੋਂ ਤੱਕ ਕਿ ਰਿਸ਼ਤੇਦਾਰ, ਦੇਸਤ ਜਾਂ ਕਸਟਮਰ ਕੇਅਰ ਨਾਲ ਕਦੇ ਵੀ ਸਾਂਝਾ ਨਹੀਂ ਕਰਨਾ ਚਾਹੀਦਾ। ਠੱਗ ਅਕਸਰ ਫੋਨ ਕਰਕੇ ਕਸਟਮਰ ਕੇਅਰ ਬਣਕੇ OTP ਮੰਗਦੇ ਹਨ, ਜੋ ਕਿ 100% ਧੋਖਾ ਹੁੰਦਾ ਹੈ।

Bank ਜਾਣਕਾਰੀ ਜਿਵੇਂ Account Number, ATM Card Number, PIN, CVV, UPI PIN ਆਦਿ ਬਹੁਤ ਗੁਪਤ ਹੁੰਦੇ ਹਨ। ਇਹ ਸਾਂਝੇ ਕਰਨ ਨਾਲ ਪੈਸੇ ਤੁਰੰਤ ਚੋਰੀ ਹੋ ਸਕਦੇ ਹਨ। ਬੈਂਕ ਕਦੇ ਵੀ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਫੋਨ, SMS ਜਾਂ ਇਮੇਲ ਰਾਹੀਂ ਨਹੀਂ ਮੰਗਦਾ।

ਸੰਖੇਪ ਵਿੱਚ, Aadhaar, School ID, OTP ਅਤੇ Bank ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ ਕਰਨਾ ਡਿਜ਼ੀਟਲ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਸਭ ਤੋਂ ਲਾਜ਼ਮੀ ਕਦਮ ਹੈ। ਹਮੇਸ਼ਾਂ ਸਚੇਤ ਰਹੋ ਅਤੇ ਆਪਣੀ ਜਾਣਕਾਰੀ ਕਿਸੇ ਨਾਲ ਵੀ ਬਿਨਾਂ ਪੁਸ਼ਟੀ ਸਾਂਝੀ ਨਾ ਕਰੋ।

9. ਮੋਬਾਈਲ ਫੋਨ ਸੁਰੱਖਿਆ ਬਾਰੇ ਜਾਣਕਾਰੀ

ਮੋਬਾਈਲ ਫੋਨ ਅੱਜਕੱਲ੍ਹ ਹਰ ਵਿਅਕਤੀ ਦੀ ਜ਼ਿੰਦਗੀ ਦਾ ਜ਼ਰੂਰੀ ਹਿੱਸਾ ਬਣ ਚੁੱਕਾ ਹੈ। ਇਹ ਸਿਰਫ਼ ਸੰਚਾਰ ਦਾ ਸਾਧਨ ਨਹੀਂ ਹੈ, ਬਲਕਿ ਬੈਂਕਿੰਗ, ਖਰੀਦਦਾਰੀ, ਸਿੱਖਿਆ ਅਤੇ ਮਨੋਰੰਜਨ ਲਈ ਵੀ ਵਰਤਿਆ ਜਾਂਦਾ ਹੈ। ਇਸ ਲਈ ਮੋਬਾਈਲ ਫੋਨ ਦੀ ਸੁਰੱਖਿਆ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਕਿਉਂਕਿ ਇਸ ਵਿੱਚ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, OTP, ਬੈਂਕ ਜਾਣਕਾਰੀ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤਿਆਂ ਦੀ ਜਾਣਕਾਰੀ ਸੁਰੱਖਿਅਤ ਹੁੰਦੀ ਹੈ।

1. ਮੋਬਾਈਲ ਸੁਰੱਖਿਆ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ **ਪਾਸਵਰਡ, ਪਿੰਨ ਅਤੇ ਫਿੰਗਰਪ੍ਰਿੰਟ ਲਾਕ** ਵਰਤੋ। ਇਹ ਤੁਹਾਡੇ ਫੋਨ ਨੂੰ ਅਣਚਾਹੇ ਵਰਤੋਂਕਾਰਾਂ ਤੋਂ ਬਚਾਉਂਦਾ ਹੈ।
2. ਮੋਬਾਈਲ ਵਿੱਚ **ਐਂਟੀਵਾਇਰਸ ਅਤੇ ਸੁਰੱਖਿਆ ਐਪਸ** ਇੰਸਟਾਲ ਕਰੋ ਅਤੇ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਅਪਡੇਟ ਕਰਦੇ ਰਹੋ।
3. **ਅਣਜਾਣ ਐਪਸ ਅਤੇ ਵੈਬਸਾਈਟਾਂ ਤੋਂ ਬਚੋ**, ਕਿਉਂਕਿ ਉਹ ਮਾਲਵੇਅਰ, ਵਾਇਰਸ ਜਾਂ ਫਰਾਡ ਦੇ ਯਤਨ ਕਰ ਸਕਦੀਆਂ ਹਨ।
4. **OTP, ਪਾਸਵਰਡ, ਬੈਂਕ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝੀ ਨਾ ਕਰੋ**, ਭਾਵੇਂ ਉਹ ਰਿਸ਼ਤੇਦਾਰ, ਦੋਸਤ ਜਾਂ ਫੋਨ ਕਾਲ ਵਿੱਚ ਕਸਟਮਰ ਕੇਅਰ ਬਣਕੇ ਪੁੱਛ ਰਿਹਾ ਹੋਵੇ।
5. **ਪਬਲਿਕ Wi-Fi ਤੋਂ ਬਿਨਾਂ VPN ਵਰਤੋਂ ਤੋਂ ਬਚੋ**, ਕਿਉਂਕਿ ਹੈਕਰ ਤੁਹਾਡਾ ਡਾਟਾ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ।
6. ਮੋਬਾਈਲ ਨੂੰ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਅਪਡੇਟ ਕਰੋ ਤਾਂ ਕਿ ਨਵੀਂ ਸੁਰੱਖਿਆ ਫੀਚਰਜ਼ ਲਾਗੂ ਹੋ ਸਕਣ।



ਸਕ੍ਰੀਨ ਲੋਕ

ਮੋਬਾਈਲ ਫੋਨ ਵਿੱਚ ਸਕ੍ਰੀਨ ਲੋਕ ਲਾਉਣਾ ਤੁਹਾਡੇ ਨਿੱਜੀ ਡਾਟਾ, ਬੈਂਕ ਜਾਣਕਾਰੀ, OTP ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਸਕ੍ਰੀਨ ਲੋਕ ਨਾ ਹੋਣ ਨਾਲ ਕੋਈ ਵੀ ਅਣਚਾਹਾ ਵਿਅਕਤੀ ਤੁਹਾਡਾ ਫੋਨ ਖੋਲ੍ਹ ਸਕਦਾ ਹੈ ਅਤੇ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ। ਇਸ ਲਈ ਮੋਬਾਈਲ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਣ ਲਈ ਕੁਝ ਮਿਹਤਵਪੂਰਨ tips ਹਨ।

1. **ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ, ਪਿੰਨ ਜਾਂ pattern ਲਾਗੂ ਕਰੋ।** Pattern ਬਣਾਉਂਦੇ ਸਮੇਂ ਆਮ ਸਧਾਰਨ shapes ਨਾ ਵਰਤੋ, ਜਿਵੇਂ ਸਿੱਧੀ ਲਕੀਰਾਂ ਜਾਂ ਆਮ ਨੰਬਰ।
2. **ਫਿੰਗਰਪ੍ਰਿੰਟ ਜਾਂ ਫੇਸ ਆਈਡੀ ਵਰਤੋਂ।** ਇਹ ਤਕਨੀਕ ਬਹੁਤ ਸੁਰੱਖਿਅਤ ਹੈ ਅਤੇ ਤੇਜ਼ੀ ਨਾਲ ਲਾਗੂ ਕਰਨ ਦੀ ਸਹੂਲਤ ਦਿੰਦੀ ਹੈ।
3. **ਸਕ੍ਰੀਨ ਆਏ-ਲੋਕ ਸਮਾਂ ਘੱਟ ਕਰੋ,** ਤਾਂ ਜੋ ਫੋਨ ਨਾ ਵਰਤਣ ਤੇ ਤੇਜ਼ੀ ਨਾਲ ਲੋਕ ਹੋ ਜਾਵੇ।
4. **ਸਕ੍ਰੀਨ ਲੋਕ ਸਕ੍ਰੀਨ 'ਤੇ ਕਿਸੇ ਨਿੱਜੀ ਪਾਸਵਰਡ ਜਾਂ PIN ਨੂੰ ਨਾ ਲਿਖੋ,** ਕਿਉਂਕਿ ਇਹ ਸੁਰੱਖਿਆ ਖਤਰੇ ਵਿੱਚ ਪਾ ਸਕਦਾ ਹੈ।
5. **ਮੋਬਾਈਲ ਨੂੰ ਅਣਜਾਣ ਲੋਕਾਂ ਨੂੰ ਦੇਖਣ ਜਾਂ ਛੂਹਣ ਤੋਂ ਬਚਾਓ।** ਛੇਵਾਂ, ਜੇ ਫੋਨ ਖੋ ਜਾਵੇ, ਤਾਂ Find My Device ਜਾਂ Similar Tracking Feature ਐਕਟਿਵ ਕਰੋ, ਜਿਸ ਨਾਲ ਤੁਸੀਂ ਡਿਵਾਈਸ ਲੱਭ ਸਕਦੇ ਹੋ ਅਤੇ ਡਾਟਾ ਸੁਰੱਖਿਅਤ ਕਰ ਸਕਦੇ ਹੋ।

ਇਹ ਸਭ ਟਿਪਸ ਅਪਣਾਉਣ ਨਾਲ ਮੋਬਾਈਲ ਸਕ੍ਰੀਨ ਲੋਕ ਮਜ਼ਬੂਤ ਬਣਦਾ ਹੈ ਅਤੇ ਤੁਹਾਡਾ ਡਿਜ਼ੀਟਲ ਡਾਟਾ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦਾ ਹੈ।

ਸੁਰੱਖਿਅਤ ਐਪ ਇੰਸਟਾਲੇਸ਼ਨ

ਮੋਬਾਈਲ ਜਾਂ ਟੈਬਲੈਟ 'ਤੇ ਐਪ ਇੰਸਟਾਲ ਕਰਨ ਸਮੇਂ ਸੁਰੱਖਿਆ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਬਿਨਾਂ ਸੁਰੱਖਿਆ ਦੇ ਇੰਸਟਾਲ ਕੀਤੇ ਗਏ ਐਪਸ ਮਾਲਵੇਅਰ, ਵਾਇਰਸ ਜਾਂ ਸਾਇਬਰ ਅਟੈਕ ਦਾ ਕਾਰਨ ਬਣ ਸਕਦੇ ਹਨ। ਇਸ ਲਈ ਹਮੇਸ਼ਾਂ **ਭਰੋਸੇਮੰਦ ਸਰੋਤਾਂ ਤੋਂ ਐਪ ਡਾਊਨਲੋਡ ਕਰੋ**, ਜਿਵੇਂ ਕਿ Google Play Store ਜਾਂ Apple App Store, ਅਣਜਾਣ ਵੈਬਸਾਈਟਾਂ, ਥਰਡ-ਪਾਰਟੀ ਸਾਈਟਾਂ ਜਾਂ ਕਿਸੇ ਅਣਪਛਾਤੇ ਲਿੰਕ ਤੋਂ ਐਪ ਡਾਊਨਲੋਡ ਨਾ ਕਰੋ।

1. ਇੰਸਟਾਲੇਸ਼ਨ ਤੋਂ ਪਹਿਲਾਂ, **ਐਪ ਦੀ ਰਿਵਿਊਜ਼ ਅਤੇ ਰੇਟਿੰਗਜ਼** ਚੈੱਕ ਕਰੋ। ਜੇ ਐਪ ਦੇ ਬਾਰੇ ਨਕਾਰਾਤਮਕ ਜਾਂ ਸੰਦੇਹਪੂਰਕ ਫੀਡਬੈਕ ਮਿਲੇ, ਤਾਂ ਉਸਨੂੰ ਇੰਸਟਾਲ ਨਾ ਕਰੋ।
2. **ਐਪ ਨੂੰ ਜੋ permissions ਮੰਗਦੀ ਹੈ, ਉਹ ਧਿਆਨ ਨਾਲ ਦੇਖੋ।** ਜੇ ਕਿਸੇ ਸਧਾਰਨ ਐਪ ਲਈ ਬੇਹਦ ਨਿੱਜੀ ਜਾਂ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਮੰਗੀ ਜਾ ਰਹੀ ਹੈ, ਤਾਂ ਇਸਨੂੰ ਇੰਸਟਾਲ ਨਾ ਕਰੋ।

ਤੁਹਾਡੇ ਫੋਨ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਣ ਲਈ, **ਐਪਸ ਨੂੰ ਨਿਯਮਿਤ ਅਪਡੇਟ ਕਰੋ**, ਕਿਉਂਕਿ ਨਵੀਆਂ ਵਰਜ਼ਨ ਵਿੱਚ ਸੁਰੱਖਿਆ ਫੀਚਰ ਸ਼ਾਮਲ ਹੁੰਦੇ ਹਨ। ਇੰਸਟਾਲ ਕਰਨ ਤੋਂ ਬਾਅਦ, ਐਂਟੀਵਾਇਰਸ ਐਪ ਜਾਂ ਸੁਰੱਖਿਆ ਐਪ ਵਰਤੋ, ਜੋ ਮਾਲਵੇਅਰ ਜਾਂ ਮਲਵੇਅਰ ਐਪਸ ਦੀ ਜਾਂਚ ਕਰ ਸਕੇ।

ਸੁਰੱਖਿਅਤ ਐਪ ਇੰਸਟਾਲੇਸ਼ਨ ਨਾਲ ਨਾ ਸਿਰਫ਼ ਤੁਹਾਡਾ ਡਿਜ਼ਿਟਲ ਡਾਟਾ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦਾ ਹੈ, ਬਲਕਿ ਮੋਬਾਈਲ ਦੀ ਕਾਰਗੁਜ਼ਾਰੀ ਵੀ ਬਿਹਤਰ ਰਹਿੰਦੀ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਸਾਵਧਾਨੀ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਐਪ ਵਰਤਣਾ ਸਭ ਤੋਂ ਸੁਰੱਖਿਅਤ ਡਿਜ਼ਿਟਲ ਆਦਤ ਹੈ।

ਐਪ ਪਰਮੀਸ਼ਨਾਂ ਦੀ ਜਾਂਚ

ਮੋਬਾਈਲ ਐਪ ਇੰਸਟਾਲ ਕਰਦਿਆਂ **ਐਪ ਪਰਮੀਸ਼ਨਾਂ ਦੀ ਜਾਂਚ** ਕਰਨਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਹਰ ਐਪ ਨੂੰ ਇੰਸਟਾਲ ਕਰਨ ਸਮੇਂ ਕੁਝ ਪਰਮੀਸ਼ਨ ਮੰਗੇ ਜਾਂਦੇ ਹਨ, ਜਿਵੇਂ ਕਿ ਕੈਮਰਾ, ਮਾਈਕ੍ਰੋਫੋਨ, ਸਟੋਰੇਜ, ਲੋਕੇਸ਼ਨ ਜਾਂ ਸੰਪਰਕਾਂ ਤੱਕ ਪਹੁੰਚ। ਇਹ ਪਰਮੀਸ਼ਨ ਐਪ ਦੀ ਕਾਰਗੁਜ਼ਾਰੀ ਲਈ ਕਈ ਵਾਰ ਲਾਜ਼ਮੀ ਹੁੰਦੇ ਹਨ, ਪਰ ਕਈ ਵਾਰੀ ਐਪ ਅਣਜਾਣ ਜਾਣਕਾਰੀ ਇਕੱਠੀ ਕਰਨ ਲਈ ਬਿਨਾਂ ਲੋੜ ਦੇ ਪਰਮੀਸ਼ਨਾਂ ਮੰਗ ਸਕਦਾ ਹੈ। ਇਸ ਲਈ ਇੰਸਟਾਲ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਇਹ ਧਿਆਨ ਨਾਲ ਵੇਖਣਾ ਚਾਹੀਦਾ ਹੈ।

1. ਸਭ ਤੋਂ ਪਹਿਲਾਂ, ਸੋਚੋ ਕਿ ਐਪ ਦੀ ਸਰਵਿਸ ਲਈ ਕੀ ਕਿਹੜੀਆਂ ਪਰਮੀਸ਼ਨਾਂ ਸਹੀ ਹਨ। ਉਦਾਹਰਨ ਲਈ, ਸਟੈਪ ਕੋਂਟਰ ਐਪ ਨੂੰ ਲੋਕੇਸ਼ਨ ਦੀ ਜ਼ਰੂਰਤ ਹੈ, ਪਰ ਕੈਮਰਾ ਜਾਂ ਸੰਪਰਕਾਂ ਦੀ ਨਹੀਂ। ਜੇ ਐਪ ਬੇਹਦ ਨਿੱਜੀ ਜਾਂ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਮੰਗਦਾ ਹੈ, ਤਾਂ ਇਸ ਨੂੰ ਇੰਸਟਾਲ ਨਾ ਕਰੋ।
2. **ਐਪ ਸੈਟਿੰਗਸ ਵਿੱਚ ਪਰਮੀਸ਼ਨਾਂ ਨੂੰ ਕੰਟਰੋਲ ਕਰੋ**, ਅਤੇ ਬਿਨਾਂ ਲੋੜੇ ਐਕਸੈਸ ਬੰਦ ਕਰੋ।

ਇਹ ਸਾਵਧਾਨੀ ਤੁਹਾਡੇ ਨਿੱਜੀ ਡਾਟਾ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਦੀ ਹੈ, ਮਾਲਵੇਅਰ ਅਤੇ ਫਰਾਡ ਤੋਂ ਬਚਾਉਂਦੀ ਹੈ, ਅਤੇ ਫੋਨ ਦੀ ਕਾਰਗੁਜ਼ਾਰੀ ਤੇ ਵੀ ਕੋਈ ਖ਼ਤਰਾ ਨਹੀਂ ਪਾਉਂਦੀ। ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਪਰਮੀਸ਼ਨਾਂ ਚੈੱਕ ਕਰਦੇ ਰਹਿਣਾ ਇੱਕ ਸੁਰੱਖਿਅਤ ਡਿਜ਼ਿਟਲ ਆਦਤ ਹੈ।

10. ਜਾਣੇ ਅਣਜਾਣੇ ਵਿੱਚ ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਗਲਤ ਜਾਣਕਾਰੀ ਸਾਂਝਾ ਕਰਨ ਸਬੰਧੀ ਜਾਗਰੂਕਤਾ

ਅੱਜਕੱਲ੍ਹ ਇੰਟਰਨੈੱਟ ਅਤੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੇ ਯੁੱਗ ਵਿੱਚ ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਗਲਤ ਜਾਣਕਾਰੀ ਇੱਕ ਵੱਡਾ ਸਮੱਸਿਆ ਬਣ ਗਈ ਹੈ। ਨਕਲੀ ਖਬਰਾਂ ਨੂੰ ਅਕਸਰ ਇਸ ਤਰ੍ਹਾਂ ਬਣਾਇਆ ਜਾਂਦਾ ਹੈ ਕਿ ਉਹ ਸੱਚ ਵਾਂਗ ਲੱਗਣ, ਪਰ ਅਸਲ ਵਿੱਚ ਇਹ ਝੂਠੀਆਂ ਜਾਂ ਧੋਖੇਬਾਜ਼ ਖਬਰਾਂ ਹੁੰਦੀਆਂ ਹਨ। ਇਹ ਖਬਰਾਂ ਕਈ ਵਾਰ ਲੋਕਾਂ ਨੂੰ ਭਰਮਿਤ ਕਰਦੀਆਂ ਹਨ, ਡਰ ਜਾਂ ਘਬਰਾਹਟ ਫੈਲਾਉਂਦੀਆਂ ਹਨ ਅਤੇ ਸਮਾਜ ਵਿੱਚ ਅਨਰਥ ਪੈਦਾ ਕਰ ਸਕਦੀਆਂ ਹਨ।



ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਗਲਤ ਜਾਣਕਾਰੀ ਤੋਂ ਬਚਣ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ ਖਬਰ ਦੇ ਸਰੋਤ ਦੀ ਜਾਂਚ ਕਰੋ। ਜਿਹੜਾ ਵੀ ਆਰਟੀਕਲ ਜਾਂ ਪੋਸਟ ਤੁਹਾਨੂੰ ਮਿਲੇ, ਉਸਦੀ ਭਰੋਸੇਮੰਦ ਵੈਬਸਾਈਟ ਜਾਂ ਸਰਕਾਰੀ ਸਰੋਤ ਨਾਲ ਪੁਸ਼ਟੀ ਕਰੋ।

ਇਸ ਤੋਂ ਇਲਾਵਾ **ਖਬਰ ਦੀ ਤਾਰੀਖ ਅਤੇ ਲੇਖਕ ਜਾਣਕਾਰੀ ਵੇਖੋ**, ਕਿਉਂਕਿ ਕਈ ਵਾਰ ਪੁਰਾਣੀ ਖਬਰਾਂ ਜਾਂ ਕਹਾਣੀਆਂ ਨੂੰ ਨਵੇਂ ਸਿਰੇ ਨਾਲ ਫੈਲਾਇਆ ਜਾਂਦਾ ਹੈ।

ਇਸ ਦੇ ਨਾਲ ਹੀ **ਸਿਰਲੇਖ ਦੇ ਚਮਕਦਾਰ ਸ਼ਬਦਾਂ ਤੇ ਨਿਰਭਰ ਨਾ ਰਹੋ**, ਕਿਉਂਕਿ ਕਈ ਵਾਰ ਇਹ ਤੁਹਾਡੇ ਦਿਲਚਸਪੀ ਖਿੱਚਣ ਲਈ exaggerated ਹੁੰਦੇ ਹਨ।

ਨਕਲੀ ਖਬਰਾਂ ਫੈਲਾਉਣ ਨਾਲ ਸਿਰਫ ਅਸਲ ਜਾਣਕਾਰੀ ਨੂੰ ਨੁਕਸਾਨ ਨਹੀਂ ਪਹੁੰਚਦਾ, ਬਲਕਿ ਸਾਈਬਰ ਧੋਖਾ ਅਤੇ ਫਰਾਡ ਦਾ ਖਤਰਾ ਵੀ ਵੱਧਦਾ ਹੈ। ਇਸ ਲਈ ਹਮੇਸ਼ਾਂ **ਸਾਵਧਾਨ, ਨਿਰਭਰਯੋਗ ਅਤੇ ਤਤਕਾਲ ਜਾਣਕਾਰੀ ਦੀ ਪੁਸ਼ਟੀ** ਕਰਕੇ ਹੀ ਕਿਸੇ ਵੀ ਖਬਰ ਜਾਂ ਜਾਣਕਾਰੀ ਨੂੰ ਸਾਂਝਾ ਕਰੋ। ਇਹ ਸੁਰੱਖਿਅਤ ਡਿਜਿਟਲ ਵਰਤੋਂ ਅਤੇ ਸਮਾਜਿਕ ਜ਼ਿੰਮੇਵਾਰੀ ਦੋਹਾਂ ਲਈ ਜ਼ਰੂਰੀ ਹੈ।

ਗਲਤ ਖਬਰਾਂ ਦੀ ਪਛਾਣ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਨਕਲੀ ਖਬਰਾਂ ਤੇ ਗਲਤ ਜਾਣਕਾਰੀ ਦਾ ਖਤਰਾ ਵੱਧ ਗਿਆ ਹੈ। ਇਸ ਲਈ ਇਹ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਅਸੀਂ ਖਬਰਾਂ ਦੀ ਸਹੀ ਪਛਾਣ ਕਰਨਾ ਸਿੱਖੀਏ। ਸਭ ਤੋਂ ਪਹਿਲਾਂ, **ਖਬਰ ਦੇ ਸਰੋਤ ਨੂੰ ਚੈੱਕ ਕਰੋ**। ਭਰੋਸੇਮੰਦ ਸਰੋਤ ਜਿਵੇਂ ਸਰਕਾਰੀ ਵੈਬਸਾਈਟ, ਪ੍ਰਮਾਣਿਤ ਨਿਊਜ਼ ਪੋਰਟਲ ਜਾਂ ਮਸ਼ਹੂਰ ਖਬਰ ਏਜੰਸੀ ਤੋਂ ਖਬਰ ਆਈ ਹੈ ਕਿ ਨਹੀਂ, ਇਹ ਵੇਖਣਾ ਜ਼ਰੂਰੀ ਹੈ।



ਦੂਜਾ, **ਖਬਰ ਦੀ ਤਾਰੀਖ ਅਤੇ ਲੇਖਕ ਜਾਣਕਾਰੀ ਵੇਖੋ**। ਕਈ ਵਾਰ ਪੁਰਾਣੀ ਖਬਰਾਂ ਨੂੰ ਨਵੀਂ ਤਰੀਕੇ ਨਾਲ ਫੈਲਾਇਆ ਜਾਂਦਾ ਹੈ, ਜੋ ਲੋਕਾਂ ਨੂੰ ਗਲਤ ਫਹਿਮੀ ਵਿੱਚ ਪਾ ਸਕਦਾ ਹੈ। ਤੀਜਾ, **ਖਬਰ ਦੇ ਸਿਰਲੇਖ ਨੂੰ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹੋ**। ਕਈ ਵਾਰ sensational ਜਾਂ ਚਮਕਦਾਰ ਸਿਰਲੇਖ ਸਿਰਫ ਦਰਸ਼ਕਾਂ ਨੂੰ ਖਿੱਚਣ ਲਈ ਬਣਾਏ ਜਾਂਦੇ ਹਨ ਅਤੇ ਅਸਲ ਖਬਰ ਨਾਲ ਮੇਲ ਨਹੀਂ ਖਾਂਦੇ। ਚੌਥਾ, **ਫੈਕਟ ਚੈੱਕਿੰਗ ਵੈਬਸਾਈਟਾਂ ਵਰਤੋਂ**, ਜਿਵੇਂ Alt News, FactCheck.org, ਜਾਂ ਵੈਰੀਫਾਈਡ ਸਰੋਤ। ਇਹਨਾਂ ਤੋਂ ਤੁਸੀਂ ਜਾਣ ਸਕਦੇ ਹੋ ਕਿ ਖਬਰ ਸੱਚ ਹੈ ਜਾਂ ਝੂਠੀ। ਪੰਜਵਾਂ, **ਸਮਾਜਿਕ ਮੀਡੀਆ 'ਤੇ ਕਿਸੇ ਵੀ ਖਬਰ ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਉਸਦੀ ਪੁਸ਼ਟੀ ਕਰੋ**। ਇਹ ਟਿਪਸ ਅਪਣਾਉਣ ਨਾਲ ਤੁਸੀਂ ਨਕਲੀ ਖਬਰਾਂ ਤੋਂ ਬਚ ਸਕਦੇ ਹੋ, ਸਹੀ ਜਾਣਕਾਰੀ ਫੈਲਾ ਸਕਦੇ ਹੋ ਅਤੇ ਆਨਲਾਈਨ ਦੁਨੀਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਣ ਵਿੱਚ ਯੋਗਦਾਨ ਪਾ ਸਕਦੇ ਹੋ।

ਨਕਲੀ ਖਬਰਾਂ ਦੀ ਜਾਂਚ (Fact Checking) ਦੇ ਤਰੀਕੇ

ਆਨਲਾਈਨ ਦੁਨੀਆਂ ਵਿੱਚ ਨਕਲੀ ਖਬਰਾਂ ਫੈਲਾਉਣਾ ਆਮ ਹੋ ਗਿਆ ਹੈ, ਇਸ ਲਈ ਖਬਰਾਂ ਦੀ **ਫੈਕਟ ਚੈੱਕਿੰਗ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਸ ਲਈ ਸਭ ਤੋਂ ਪਹਿਲਾਂ,

1. **ਖਬਰ ਦੇ ਸਰੋਤ ਦੀ ਜਾਂਚ ਕਰੋ**। ਭਰੋਸੇਮੰਦ ਨਿਊਜ਼ ਪੋਰਟਲ, ਸਰਕਾਰੀ ਵੈਬਸਾਈਟ ਜਾਂ ਪ੍ਰਮਾਣਿਤ ਖਬਰ ਏਜੰਸੀ ਤੋਂ ਹੀ ਜਾਣਕਾਰੀ ਲਵੋ। ਜੇ ਖਬਰ ਅਣਜਾਣ ਵੈਬਸਾਈਟ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪੋਸਟ ਤੋਂ ਆਈ ਹੈ, ਤਾਂ ਇਸਨੂੰ ਸਿੱਧਾ ਸੱਚ ਨਹੀਂ ਮੰਨਣਾ ਚਾਹੀਦਾ।
2. **ਖਬਰ ਦੀ ਤਾਰੀਖ ਅਤੇ ਲੇਖਕ ਨੂੰ ਵੇਖੋ**। ਕਈ ਵਾਰ ਪੁਰਾਣੀਆਂ ਖਬਰਾਂ ਜਾਂ ਆਰਟੀਕਲ ਨੂੰ ਨਵੀਂ ਤਰੀਕੇ ਨਾਲ ਪੇਸ਼ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।
3. **ਖਬਰ ਦੇ ਵੇਰਵੇ ਨੂੰ ਕ੍ਰਾਸ-ਚੈੱਕ ਕਰੋ**। ਵੱਖ-ਵੱਖ ਭਰੋਸੇਮੰਦ ਸਰੋਤਾਂ ਤੋਂ ਉਸੀ ਖਬਰ ਬਾਰੇ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰੋ। ਜੇ ਵੱਖ-ਵੱਖ ਸਰੋਤ ਖਬਰ ਨੂੰ ਸਹਿਮਤ ਨਹੀਂ ਕਰਦੇ, ਤਾਂ ਇਹ ਸੰਦੇਹਪੂਰਕ ਹੈ।
4. **ਫੈਕਟ-ਚੈੱਕਿੰਗ ਵੈਬਸਾਈਟਾਂ ਵਰਤੋਂ**, ਜਿਵੇਂ Alt News, Boom Live, FactCheck.org ਜਾਂ Indigenous Fact Check Websites। ਇਹ ਸਾਈਟਾਂ ਖਬਰਾਂ ਦੀ ਸਹੀ ਜਾਂ ਝੂਠੀ ਹੋਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰਦੀਆਂ ਹਨ।
5. **ਚਮਕਦਾਰ ਸਿਰਲੇਖ ਤੇ ਨਿਰਭਰ ਨਾ ਰਹੋ**, ਕਿਉਂਕਿ ਕਈ ਵਾਰ ਇਹ ਸਿਰਫ ਲੋਕਾਂ ਦੀ ਧਿਆਨ ਖਿੱਚਣ ਲਈ ਬਣਾਏ ਜਾਂਦੇ ਹਨ।

ਫੈਕਟ ਚੈੱਕਿੰਗ ਨਾਲ ਤੁਸੀਂ ਨਕਲੀ ਖਬਰਾਂ ਤੋਂ ਬਚ ਸਕਦੇ ਹੋ ਅਤੇ ਸਹੀ ਜਾਣਕਾਰੀ ਫੈਲਾਉਣ ਵਿੱਚ ਯੋਗਦਾਨ ਪਾ ਸਕਦੇ ਹੋ।

11. ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਅਤੇ ਕਾਨੂੰਨੀ ਜਾਣਕਾਰੀ

ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਅੱਜਕੱਲ੍ਹ ਦੀ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਇੱਕ ਵੱਡੀ ਸਮੱਸਿਆ ਬਣ ਗਿਆ ਹੈ। ਇਹ ਕਿਸੇ ਵੀ ਤਰ੍ਹਾਂ ਦਾ ਅਪਰਾਧ ਹੁੰਦਾ ਹੈ ਜੋ ਕੰਪਿਊਟਰ, ਇੰਟਰਨੈੱਟ, ਮੋਬਾਈਲ ਜਾਂ ਹੋਰ ਡਿਜ਼ਿਟਲ ਡਿਵਾਈਸਾਂ ਰਾਹੀਂ ਕੀਤਾ ਜਾਂਦਾ ਹੈ। ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਵਿੱਚ ਹੈਕਿੰਗ, ਫਰਾਡ, ਫਿਸ਼ਿੰਗ, OTP ਚੋਰੀ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਬੁਲਿੰਗ, ਨਕਲੀ ਖਬਰਾਂ ਫੈਲਾਉਣਾ ਅਤੇ ਪੈਸਾ ਚੋਰੀ ਵਰਗੀਆਂ ਗਤੀਵਿਧੀਆਂ ਸ਼ਾਮਲ ਹਨ। ਇਹ ਅਪਰਾਧ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਪੈਸਾ ਅਤੇ ਸੁਰੱਖਿਆ ਲਈ ਵੱਡਾ ਖਤਰਾ ਬਣ ਸਕਦੇ ਹਨ।

ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਤੋਂ ਬਚਣ ਲਈ ਲੋਕਾਂ ਨੂੰ ਸਾਵਧਾਨ ਰਹਿਣਾ ਅਤੇ ਡਿਜ਼ਿਟਲ ਸੁਰੱਖਿਆ ਦੇ ਨਿਯਮਾਂ ਦੀ ਪਾਲਣਾ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ, ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ, ਸਕ੍ਰੀਨ ਲੋਕ, ਸੁਰੱਖਿਅਤ ਐਪ ਇੰਸਟਾਲੇਸ਼ਨ ਅਤੇ ਫੈਕਟ-ਚੈਕਿੰਗ ਵਰਗੀਆਂ ਆਦਤਾਂ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਤੋਂ ਬਚਾਉਂਦੀਆਂ ਹਨ।

ਭਾਰਤ ਵਿੱਚ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਅਤੇ ਇਸ ਨਾਲ ਜੁੜੇ ਮਾਮਲਿਆਂ ਲਈ **Indian IT Act, 2000** ਮੁੱਖ ਕਾਨੂੰਨ ਹੈ। ਇਸ ਕਾਨੂੰਨ ਅਧੀਨ ਹੈਕਿੰਗ, ਅਣਅਧਿਕਾਰਤ ਡਾਟਾ ਚੋਰੀ, ਫਰਾਡ ਅਤੇ ਈ-ਹਰਾਸਮੈਂਟ ਲਈ ਸਜ਼ਾ ਅਤੇ ਜੁਰਮਾਨਾ ਦਿੱਤਾ ਜਾ ਸਕਦਾ ਹੈ। ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਦੇ ਸ਼ਿਕਾਰ ਹੋਣ 'ਤੇ ਲੋਕ **ਪੁਲਿਸ ਸਾਈਬਰ ਸੈੱਲ** ਜਾਂ **Online Cyber Complaint Portal** ਤੇ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰ ਸਕਦੇ ਹਨ।

ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਤੋਂ ਬਚਣ ਲਈ ਸੁਰੱਖਿਆ ਦੇ ਨਿਯਮਾਂ ਦੀ ਪਾਲਣਾ ਕਰਨੀ, ਜਾਣਕਾਰੀ ਨੂੰ ਸਾਵਧਾਨੀ ਨਾਲ ਸਾਂਝੀ ਕਰਨੀ ਅਤੇ ਕਾਨੂੰਨੀ ਸਰੋਤਾਂ ਦੀ ਜਾਣਕਾਰੀ ਰੱਖਣੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਹ ਸੁਰੱਖਿਅਤ ਅਤੇ ਸੱਚੀ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂ ਲਈ ਜ਼ਰੂਰੀ ਹੈ।



IT Act 2000 ਦੀ ਬੇਸਿਕ ਜਾਣਕਾਰੀ

Information Technology Act, 2000 (ਆਈਟੀ ਐਕਟ 2000) ਭਾਰਤ ਵਿੱਚ ਇੰਟਰਨੈੱਟ ਅਤੇ ਡਿਜ਼ੀਟਲ ਦੁਨੀਆ ਨੂੰ ਨਿਯੰਤਰਿਤ ਕਰਨ ਲਈ ਬਣਾਇਆ ਗਿਆ ਮੁੱਖ ਕਾਨੂੰਨ ਹੈ। ਇਸਦਾ ਮੁੱਖ ਉਦੇਸ਼ ਡਿਜ਼ੀਟਲ ਮਾਮਲਿਆਂ ਵਿੱਚ ਸੁਰੱਖਿਆ, ਭਰੋਸੇਮੰਦ ਡਿਜ਼ੀਟਲ ਲੈਣ-ਦੇਣ ਅਤੇ ਸਾਈਬਰ ਅਪਰਾਧਾਂ ਤੋਂ ਰੋਕਥਾਮ ਕਰਨਾ ਹੈ। ਇਹ ਕਾਨੂੰਨ 17 ਅਕਤੂਬਰ, 2000 ਨੂੰ ਲਾਗੂ ਹੋਇਆ ਅਤੇ ਇਸ ਨੂੰ ਬਾਅਦ ਵਿੱਚ ਵੱਖ-ਵੱਖ ਤਰੀਕਿਆਂ ਨਾਲ ਅਪਡੇਟ ਕੀਤਾ ਗਿਆ।

IT Act 2000 ਦੇ ਤਹਿਤ, ਕਿਸੇ ਵੀ ਹੈਕਿੰਗ, ਡਾਟਾ ਚੋਰੀ, ਫਰਾਡ, ਫਿਸ਼ਿੰਗ, ਆਨਲਾਈਨ ਹੱਰਾਸਮੈਂਟ, ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਪੂਰਨ ਜਾਂ ਅਣਪੂਰਨ ਡਿਜ਼ੀਟਲ ਦਸਤਾਵੇਜ਼ਾਂ ਦੀ ਬਣਾਵਟ ਅਪਰਾਧ ਮੰਨੀ ਜਾਂਦੀ ਹੈ। ਇਹ ਕਾਨੂੰਨ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਲਈ ਸਜ਼ਾ ਅਤੇ ਜੁਰਮਾਨੇ ਦਾ ਪ੍ਰਬੰਧ ਕਰਦਾ ਹੈ। ਉਦਾਹਰਨ ਲਈ, ਹੈਕਿੰਗ, ਅਣਅਧਿਕਾਰਤ ਡਾਟਾ ਤਬਦੀਲ ਕਰਨਾ ਜਾਂ ਪੈਸਾ ਚੋਰੀ ਕਰਨ ਵਾਲਿਆਂ ਨੂੰ ਸਜ਼ਾ ਮਿਲ ਸਕਦੀ ਹੈ।

ਇਸ ਕਾਨੂੰਨ ਨੇ ਡਿਜ਼ੀਟਲ ਸਿਗਨੇਚਰ, ਈ-ਕੰਮਰਸ ਅਤੇ ਈ-ਗਵਰਨੈਂਸ ਸਿਸਟਮਾਂ ਨੂੰ ਕਾਨੂੰਨੀ ਮਾਨਤਾ ਦਿੱਤੀ। ਇਹ ਡਿਜ਼ੀਟਲ ਦਸਤਾਵੇਜ਼ਾਂ ਅਤੇ ਈ-ਕੰਮਰਸ ਲੈਣ-ਦੇਣ ਨੂੰ ਭਰੋਸੇਮੰਦ ਬਣਾਉਂਦਾ ਹੈ। IT Act ਦੇ ਤਹਿਤ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੇ ਮਾਮਲੇ ਲਈ ਪੁਲਿਸ ਸਾਈਬਰ ਸੈੱਲ ਦਾ ਸਥਾਪਨ ਕੀਤਾ ਗਿਆ ਹੈ, ਜਿੱਥੇ ਲੋਕ ਸਾਈਬਰ ਧੋਖਾਧੜੀ ਜਾਂ ਫਰਾਡ ਦੀ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰ ਸਕਦੇ ਹਨ।

ਇਸ ਕਾਨੂੰਨ ਦੀ ਜਾਣਕਾਰੀ ਰੱਖਣਾ ਹਰ ਡਿਜ਼ੀਟਲ ਉਪਭੋਗਤਾ ਲਈ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਸ ਨਾਲ ਲੋਕ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਮਾਲੀ ਜਾਣਕਾਰੀ ਅਤੇ ਡਿਜ਼ੀਟਲ ਹੱਕਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹਨ। ਸੰਖੇਪ ਵਿੱਚ, IT Act 2000 ਭਾਰਤ ਵਿੱਚ ਡਿਜ਼ੀਟਲ ਸੁਰੱਖਿਆ, ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਅਤੇ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਰੋਕਥਾਮ ਲਈ ਅਤਿ ਜ਼ਰੂਰੀ ਕਾਨੂੰਨ ਹੈ।

ਬੱਚਿਆਂ ਖ਼ਿਲਾਫ਼ ਆਨਲਾਈਨ ਅਪਰਾਧ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਬੱਚਿਆਂ ਲਈ ਸਿੱਖਣ ਅਤੇ ਮਨੋਰੰਜਨ ਦਾ ਸਾਧਨ ਹੈ, ਪਰ ਇਸ ਨਾਲ ਉਹਨਾਂ ਨੂੰ ਸਾਈਬਰ ਅਪਰਾਧਾਂ ਦਾ ਖ਼ਤਰਾ ਵੀ ਵੱਧ ਜਾਂਦਾ ਹੈ। ਬੱਚਿਆਂ ਖ਼ਿਲਾਫ਼ ਆਨਲਾਈਨ ਅਪਰਾਧ ਵਿੱਚ ਸਾਈਬਰ ਬੁਲਿੰਗ, ਸੈਕਸੁਅਲ ਹੱਰਾਸਮੈਂਟ, ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਚੈਟ, ਨਾਜਾਇਜ਼ ਸਮੱਗਰੀ ਭੇਜਣਾ, ਫਰਾਡ ਅਤੇ ਪਛਾਣ ਚੋਰੀ ਸ਼ਾਮਲ ਹਨ। ਕਈ ਵਾਰ

ਬੱਚੇ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਫੋਟੋ ਜਾਂ ਵੀਡੀਓ ਬਿਨਾਂ ਸਾਵਧਾਨੀ ਦੇ ਸਾਂਝੇ ਕਰ ਦਿੰਦੇ ਹਨ, ਜੋ ਕਿ ਅਪਰਾਧੀਆਂ ਲਈ ਫਾਇਦਾ ਬਣ ਸਕਦਾ ਹੈ।

ਸਾਈਬਰ ਬੁਲਿੰਗ ਅਤੇ ਹੈਰਾਸਮੈਂਟ ਬੱਚਿਆਂ ਦੀ **ਮਨੋਵਿਗਿਆਨਿਕ ਸਿਹਤ** 'ਤੇ ਨਕਾਰਾਤਮਕ ਪ੍ਰਭਾਵ ਪਾ ਸਕਦਾ ਹੈ, ਜਿਸ ਨਾਲ ਉਹ ਡਿੱਗਣ, ਡਰਣਾ ਜਾਂ ਖੁਦ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਦੇ ਖਤਰੇ ਵਿੱਚ ਆ ਸਕਦੇ ਹਨ। ਇਸ ਲਈ, ਬੱਚਿਆਂ ਨੂੰ **ਸੁਰੱਖਿਅਤ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂ ਅਤੇ ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ** ਦੀ ਸਿੱਖਿਆ ਦੇਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਮਾਪੇ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਚਾਹੀਦਾ ਹੈ ਕਿ ਉਹ ਬੱਚਿਆਂ ਦੀ **ਮੋਬਾਈਲ ਅਤੇ ਕੰਪਿਊਟਰ ਐਕਟਿਵਿਟੀ** 'ਤੇ ਨਜ਼ਰ ਰੱਖਣ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਅਣਜਾਣ ਲਿੰਕਾਂ, ਅਣਜਾਣ ਲੋਕਾਂ ਅਤੇ ਨਾਜਾਇਜ਼ ਸਮੱਗਰੀ ਤੋਂ ਸੁਰੱਖਿਅਤ ਰੱਖਣ। ਸੁਰੱਖਿਆਵਾਂ ਨਾਲ, ਬੱਚੇ ਆਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿ ਸਕਦੇ ਹਨ ਅਤੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਦਾ ਸਹੀ ਤਰੀਕੇ ਨਾਲ ਲੁਤਫ਼ ਲੈ ਸਕਦੇ ਹਨ।

ਕਿੱਥੇ ਰਿਪੋਰਟ ਕਰਨਾ ਹੈ (Cyber Crime Portal, 1930 Helpline)

ਆਨਲਾਈਨ ਦੁਨੀਆਂ ਦੇ ਵਧਦੇ ਖਤਰਾ ਅਤੇ ਸਾਈਬਰ ਅਪਰਾਧਾਂ ਦੇ ਕਾਰਨ, ਭਾਰਤ ਸਰਕਾਰ ਨੇ ਲੋਕਾਂ ਲਈ ਸੁਰੱਖਿਆ ਅਤੇ ਰਿਪੋਰਟਿੰਗ ਸਿਸਟਮ ਬਣਾਇਆ ਹੈ। ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਦੀ ਰਿਪੋਰਟਿੰਗ ਕਰਨ ਦੇ ਮੁੱਖ ਤਰੀਕੇ ਹਨ: **National Cyber Crime Reporting Portal** <https://cybercrime.gov.in> ਅਤੇ **1930 Helpline**

ਇਹ ਦੋਹਾਂ ਸਰਕਾਰੀ ਸਰੋਤ ਹਨ ਜੋ ਸਾਈਬਰ ਧੋਖਾਧੜੀ, ਬੁਲਿੰਗ, ਫਰਾਡ, ਹੈਕਿੰਗ ਅਤੇ ਬੱਚਿਆਂ ਖਿਲਾਫ਼ ਅਪਰਾਧਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਵਿੱਚ ਸਹਾਇਕ ਹਨ।

1. National Cyber Crime Reporting Portal:

ਇਹ ਪੋਰਟਲ ਭਾਰਤ ਸਰਕਾਰ ਅਤੇ Ministry of Home Affairs ਦੁਆਰਾ ਬਣਾਇਆ ਗਿਆ ਹੈ। ਇਸਦਾ ਉਦੇਸ਼ ਹੈ ਕਿ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਦੇ ਮਾਮਲਿਆਂ ਨੂੰ ਆਸਾਨੀ ਨਾਲ ਰਿਪੋਰਟ ਕੀਤਾ ਜਾ ਸਕੇ। ਪੋਰਟਲ ਦੇ ਮਾਧਿਅਮ ਨਾਲ ਵਿਅਕਤੀ ਕਈ ਕਿਸਮ ਦੇ ਸਾਈਬਰ ਅਪਰਾਧਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰ ਸਕਦਾ ਹੈ, ਜਿਵੇਂ ਕਿ:

- ਬੱਚਿਆਂ ਖਿਲਾਫ਼ ਪੇਰਨੇਗ੍ਰਾਫੀ ਜਾਂ ਹੈਰਾਸਮੈਂਟ
- ਫਰਾਡ ਅਤੇ ਫਿਸ਼ਿੰਗ ਅਟੈਕ
- ਹੈਕਿੰਗ ਅਤੇ ਡਾਟਾ ਚੋਰੀ

- ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਮਿਸਲੈਡਿੰਗ ਜਾਣਕਾਰੀ

ਰਿਪੋਰਟ ਕਰਨ ਲਈ, ਪੋਰਟਲ 'ਤੇ **ਲਾਗਿਨ ਕਰਨਾ ਜ਼ਰੂਰੀ ਹੈ**। ਆਮ ਤੌਰ 'ਤੇ, ਰਿਪੋਰਟ ਵਿੱਚ ਆਪਣਾ ਨਾਮ, ਫੋਨ ਨੰਬਰ, ਈਮੇਲ, ਸਬੂਤ (ਸਕ੍ਰੀਨਸ਼ਾਟ, ਲਿੰਕ, ਸੰਦੇਸ਼ ਆਦਿ) ਅਤੇ ਘਟਨਾ ਦਾ ਵੇਰਵਾ ਦੇਣਾ ਪੈਂਦਾ ਹੈ। ਰਿਪੋਰਟ ਦਰਜ ਹੋਣ ਤੋਂ ਬਾਅਦ, ਪੁਲਿਸ ਜਾਂ ਸਾਈਬਰ ਸੈੱਲ ਦੁਆਰਾ ਉਸਦੀ ਜਾਂਚ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।

2. 1930 Helpline:

1930 Helpline ਖਾਸ ਤੌਰ 'ਤੇ ਬੱਚਿਆਂ ਖਿਲਾਫ਼ ਆਨਲਾਈਨ ਅਪਰਾਧਾਂ ਲਈ ਹੈ। ਇਹ Helpline Ministry of Women and Child Development ਦੁਆਰਾ ਚਲਾਈ ਜਾਂਦੀ ਹੈ। ਇਸ 'ਤੇ ਕਾਲ ਕਰਕੇ ਕਿਸੇ ਵੀ ਬੱਚੇ ਦੀ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਮਾਮਲੇ ਦੀ ਰਿਪੋਰਟ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ। 1930 Helpline ਨਾ ਸਿਰਫ਼ ਰਿਪੋਰਟ ਲੈਂਦੀ ਹੈ, ਬਲਕਿ **ਮਦਦ ਅਤੇ ਕਾਊਂਸਲਿੰਗ ਸੇਵਾ** ਵੀ ਪ੍ਰਦਾਨ ਕਰਦੀ ਹੈ। ਇਹ Helpline ਮੁਫ਼ਤ ਹੈ ਅਤੇ ਸਮੂਹ ਭਾਰਤ ਵਿੱਚ 24×7 ਉਪਲਬਧ ਹੈ।

ਕਿਵੇਂ ਰਿਪੋਰਟ ਕਰੀਏ:

- Cyber Crime Portal: <https://cybercrime.gov.in> ਤੇ ਜਾਓ → ਆਪਣੇ ਖਾਤੇ ਨਾਲ ਲਾਗਿਨ ਕਰੋ → ਮਾਮਲੇ ਦੀ ਸ਼੍ਰੇਣੀ ਚੁਣੋ → ਘਟਨਾ ਦਾ ਵੇਰਵਾ ਅਤੇ ਸਬੂਤ ਦਿਓ → ਰਿਪੋਰਟ ਸਬਮਿਟ ਕਰੋ।
- 1930 Helpline: 1930 ਤੇ ਕਾਲ ਕਰੋ → ਮਾਮਲੇ ਦਾ ਵੇਰਵਾ ਦਿਓ → ਪ੍ਰੋਫੈਸ਼ਨਲ ਸਹਾਇਤਾ ਪ੍ਰਾਪਤ ਕਰੋ → ਜੇ ਲੋੜ ਹੋਵੇ ਤਾਂ Follow-up ਰਿਪੋਰਟਿੰਗ ਕਰੋ।

ਇਹ ਸਰਕਾਰੀ ਸਿਸਟਮਾਂ ਨਿਰਭਰਯੋਗ ਅਤੇ ਸੁਰੱਖਿਅਤ ਹਨ। ਰਿਪੋਰਟਿੰਗ ਨਾਲ ਨਾ ਸਿਰਫ਼ ਸਾਈਬਰ ਅਪਰਾਧੀਆਂ ਨੂੰ ਕਾਨੂੰਨੀ ਤੌਰ 'ਤੇ ਸਜ਼ਾ ਮਿਲਦੀ ਹੈ, ਬਲਕਿ ਲੱਖਾਂ ਲੋਕਾਂ, ਖਾਸ ਕਰਕੇ ਬੱਚਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਯਕੀਨੀ ਬਣਦੀ ਹੈ। ਇਸ ਲਈ ਹਰ ਵਿਅਕਤੀ ਨੂੰ ਚਾਹੀਦਾ ਹੈ ਕਿ ਕੋਈ ਵੀ ਸਾਈਬਰ ਅਪਰਾਧ ਦੇਖਣ ਜਾਂ ਉਸਦਾ ਸ਼ਿਕਾਰ ਹੋਣ 'ਤੇ ਤੁਰੰਤ ਰਿਪੋਰਟ ਕਰੇ।

ਇਸ ਤਰ੍ਹਾਂ, Cyber Crime Portal ਅਤੇ 1930 Helpline ਸਾਈਬਰ ਦੁਨੀਆਂ ਵਿੱਚ ਸੁਰੱਖਿਆ, ਜ਼ਿੰਮੇਵਾਰੀ ਅਤੇ ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਉਂਦੇ ਹਨ।

12. ਆਮ ਤੌਰ ਤੇ ਵਰਤੇ ਜਾਣ ਵਾਲੇ ਡਿਜੀਟਲ ਡਿਵਾਈਸਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਤਰੀਕੇ ਨਾਲ ਵਰਤਣ ਸਬੰਧੀ ਸੁਝਾਅ

ਅਤੇ ਨੈੱਟਵਰਕ ਸੁਰੱਖਿਆ

ਅੱਜ ਦੇ ਡਿਜੀਟਲ ਯੁੱਗ ਵਿੱਚ ਸਾਡੀ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਮੋਬਾਈਲ, ਟੈਬਲੈਟ, ਲੈਪਟੋਪ ਅਤੇ ਹੋਰ ਡਿਜੀਟਲ ਡਿਵਾਈਸ ਮੁੱਖ ਭੂਮਿਕਾ ਨਿਭਾ ਰਹੇ ਹਨ। ਇੰਟਰਨੈੱਟ ਅਤੇ ਨੈੱਟਵਰਕ ਸੇਵਾਵਾਂ ਦੇ ਵਧਦੇ ਵਰਤੋਂ ਨਾਲ ਡਿਜੀਟਲ ਸੁਰੱਖਿਆ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੋ ਗਈ ਹੈ। **ਡਿਵਾਈਸ ਅਤੇ ਨੈੱਟਵਰਕ ਸੁਰੱਖਿਆ** ਨਾਲ ਅਸੀਂ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਪੈਸਾ ਅਤੇ ਡਿਜੀਟਲ ਹੱਕਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹਾਂ।

ਸਭ ਤੋਂ ਪਹਿਲਾਂ, **ਡਿਵਾਈਸ ਸੁਰੱਖਿਆ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਮੋਬਾਈਲ, ਲੈਪਟੋਪ ਜਾਂ ਟੈਬਲੈਟ 'ਤੇ ਸਕ੍ਰੀਨ ਲੋਕ, ਪਾਸਵਰਡ, ਫਿੰਗਰਪ੍ਰਿੰਟ ਜਾਂ ਫੇਸ ਆਈਡੀ ਵਰਤੋਂ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਅਣਚਾਹੇ ਵਰਤੋਂਕਾਰਾਂ ਤੋਂ ਡਿਵਾਈਸ ਨੂੰ ਬਚਾਉਂਦਾ ਹੈ। ਸਾਥ ਹੀ, ਡਿਵਾਈਸ 'ਤੇ ਸਿਰਫ਼ ਭਰੋਸੇਮੰਦ ਸਰੋਤਾਂ ਤੋਂ ਐਪਸ ਇੰਸਟਾਲ ਕਰੋ ਅਤੇ **ਐਪ ਪਰਮੀਸ਼ਨਾਂ** ਨੂੰ ਧਿਆਨ ਨਾਲ ਚੈੱਕ ਕਰੋ। ਡਿਵਾਈਸ ਅਤੇ ਐਪਸ ਨੂੰ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਅਪਡੇਟ ਕਰਦੇ ਰਹੋ ਤਾਂ ਕਿ ਨਵੀਂ ਸੁਰੱਖਿਆ ਫੀਚਰਜ਼ ਲਾਗੂ ਹੋ ਸਕਣ।



ਦੂਜਾ, **ਨੈੱਟਵਰਕ ਸੁਰੱਖਿਆ** ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਪਬਲਿਕ Wi-Fi ਤੋਂ ਬਿਨਾਂ VPN (Virtual Private Network) ਵਰਤੋਂ ਕਰੋ, ਕਿਉਂਕਿ ਹੈਕਰ ਇਸ ਰਾਹੀਂ ਤੁਹਾਡਾ ਡਾਟਾ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ। ਆਪਣੇ Wi-Fi ਰਾਊਟਰ ਦੀ ਪਾਸਵਰਡ ਸੁਰੱਖਿਅਤ ਰੱਖੋ ਅਤੇ WPA3 ਜਿਵੇਂ ਮਜ਼ਬੂਤ ਇੰਕ੍ਰਿਪਸ਼ਨ ਪ੍ਰੋਟੋਕਾਲ ਵਰਤੋਂ। ਫਾਇਰਵਾਲ ਅਤੇ ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਨਾਲ ਨੈੱਟਵਰਕ ਤੇ ਡਿਵਾਈਸ ਨੂੰ ਵਾਇਰਸ, ਮਾਲਵੇਅਰ ਅਤੇ ਹੈਕਿੰਗ ਤੋਂ ਬਚਾਇਆ ਜਾ ਸਕਦਾ ਹੈ।

ਤਿੰਜਾ, **ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ** ਸੁਰੱਖਿਆ ਦਾ ਅਹੰਸਭਾਗ ਹੈ। ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਲਿੰਕ, ਫਰਾਡਈ ਈਮੇਲ ਜਾਂ ਮੈਸੇਜ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ। ਆਪਣੇ ਪਾਸਵਰਡ, OTP, ਬੈਂਕ ਜਾਣਕਾਰੀ ਅਤੇ ਨਿੱਜੀ ਡਾਟਾ ਨੂੰ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ।

ਐਂਟੀਵਾਇਰਸ

ਅੱਜ ਦੀ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ, ਮੋਬਾਈਲ, ਲੈਪਟੋਪ ਅਤੇ ਕੰਪਿਊਟਰ ਸਾਈਬਰ ਖ਼ਤਰਾ ਤੋਂ ਬਚਾਉਣ ਲਈ **ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਐਂਟੀਵਾਇਰਸ ਇੱਕ ਪ੍ਰੋਗਰਾਮ ਹੈ ਜੋ ਤੁਹਾਡੇ ਡਿਵਾਈਸ ਨੂੰ **ਵਾਇਰਸ, ਮਾਲਵੇਅਰ, ਟਰੋਜਨ, ਸਪਾਈਵੇਅਰ ਅਤੇ ਰੈਨਸਮਵੇਅਰ** ਤੋਂ ਸੁਰੱਖਿਅਤ ਰੱਖਦਾ ਹੈ। ਇਹ ਸਾਫਟਵੇਅਰ ਮਾਲਵੇਅਰ ਦੇ ਰੂਪ ਵਿੱਚ ਆਉਣ ਵਾਲੇ ਖ਼ਤਰੇ ਦੀ ਪਛਾਣ ਕਰਦਾ ਹੈ ਅਤੇ ਉਸਨੂੰ ਹਟਾਉਂਦਾ ਹੈ।



ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਨਾਲ ਤੁਹਾਡਾ ਡਿਵਾਈਸ ਤੇਜ਼ ਅਤੇ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦਾ ਹੈ। ਇਹ **ਰੀਅਲ-ਟਾਈਮ ਸਕੈਨਿੰਗ** ਕਰਕੇ ਡਾਟਾ, ਫਾਈਲਾਂ, ਐਪਸ ਅਤੇ ਇੰਟਰਨੈੱਟ ਡਾਊਨਲੋਡ ਦੀ ਜਾਂਚ ਕਰਦਾ ਹੈ। ਜਦੋਂ ਕੋਈ ਸ਼ੱਕੀ ਫਾਈਲ ਜਾਂ ਵੈਬਸਾਈਟ ਮਿਲਦੀ ਹੈ, ਤਾਂ ਇਹ ਤੁਹਾਨੂੰ ਤੁਰੰਤ ਸੂਚਿਤ ਕਰਦਾ ਹੈ। ਇਸਦੇ ਨਾਲ ਹੀ, ਬਹੁਤ ਸਾਰੇ ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਵਿੱਚ **ਫਾਇਰਵਾਲ, ਡਾਟਾ ਇੰਕ੍ਰਿਪਸ਼ਨ ਅਤੇ ਫਿਸ਼ਿੰਗ ਸੁਰੱਖਿਆ** ਜਿਵੇਂ ਫੀਚਰ ਵੀ ਸ਼ਾਮਲ ਹੁੰਦੇ ਹਨ।

ਐਂਟੀਵਾਇਰਸ ਨੂੰ **ਨਿਯਮਤ ਅਪਡੇਟ** ਕਰਨਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਕਿਉਂਕਿ ਨਵੇਂ ਵਾਇਰਸ ਅਤੇ ਮਾਲਵੇਅਰ ਹਰ ਰੋਜ਼ ਬਣਦੇ ਰਹਿੰਦੇ ਹਨ। ਇਸਦੇ ਬਿਨਾਂ, ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਅਪਡੇਟ ਨਾ ਹੋਣ ਕਾਰਨ ਨਵੇਂ ਖਤਰਿਆਂ ਤੋਂ ਸੁਰੱਖਿਆ ਨਹੀਂ ਕਰ ਸਕਦਾ।

ਸੰਖੇਪ ਵਿੱਚ, ਐਂਟੀਵਾਇਰਸ ਡਿਵਾਈਸ ਸੁਰੱਖਿਆ ਦਾ ਮੁੱਖ ਹਿੱਸਾ ਹੈ। ਇਹ ਸਿਰਫ ਮਾਲਵੇਅਰ ਤੋਂ ਬਚਾਉਂਦਾ ਹੀ ਨਹੀਂ, ਬਲਕਿ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਬੈਂਕਿੰਗ ਡਾਟਾ ਅਤੇ ਡਿਜ਼ਿਟਲ ਡਿਵਾਈਸ ਦੀ ਕਾਰਗੁਜ਼ਾਰੀ ਨੂੰ ਵੀ ਸੁਰੱਖਿਅਤ ਰੱਖਦਾ ਹੈ। ਇਸ ਲਈ ਹਰ ਡਿਵਾਈਸ ‘ਤੇ ਮਜ਼ਬੂਤ ਅਤੇ ਨਿਯਮਤ ਅਪਡੇਟ ਐਂਟੀਵਾਇਰਸ ਲਗਾਉਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਸੁਰੱਖਿਅਤ Wi-Fi ਵਰਤੋਂ

ਅੱਜਕੱਲ੍ਹ ਇੰਟਰਨੈੱਟ ਸਾਡੀ ਜ਼ਿੰਦਗੀ ਦਾ ਅਹਿੰਸਭਾਗ ਬਣ ਗਿਆ ਹੈ। ਘਰ, ਦਫਤਰ ਅਤੇ ਪਬਲਿਕ ਥਾਵਾਂ ‘ਤੇ Wi-Fi ਦੀ ਵਰਤੋਂ ਨਾਲ ਅਸੀਂ ਬਹੁਤ ਸਾਰੀਆਂ ਗਤੀਵਿਧੀਆਂ ਕਰ ਸਕਦੇ ਹਾਂ, ਜਿਵੇਂ ਕਿ ਈ-ਮੇਲ, ਆਨਲਾਈਨ ਖਰੀਦਦਾਰੀ, ਬੈਂਕਿੰਗ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਮਨੋਰੰਜਨ। ਪਰ Wi-Fi ਦਾ ਸੁਰੱਖਿਅਤ ਨਾ ਹੋਣਾ ਸਾਈਬਰ ਖਤਰਾ ਵਧਾ ਸਕਦਾ ਹੈ। ਇਸ ਲਈ **ਸੁਰੱਖਿਅਤ Wi-Fi ਵਰਤੋਂ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

1. ਘਰ ਜਾਂ ਦਫਤਰ ਦੇ Wi-Fi ਰਾਊਟਰ ਨੂੰ **ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ** ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰੋ। ਆਮ ਪਾਸਵਰਡ ਵਰਤਣਾ, ਜਿਵੇਂ “12345678” ਜਾਂ “password,” ਹੈਕਰ ਲਈ ਆਸਾਨ ਨਿਸ਼ਾਨਾ ਬਣ ਸਕਦਾ ਹੈ। WPA3 ਜਿਵੇਂ ਮਜ਼ਬੂਤ ਇੰਕ੍ਰਿਪਸ਼ਨ ਪ੍ਰੋਟੋਕਾਲ ਵਰਤਣਾ ਵੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਜੋ ਡਾਟਾ ਨੂੰ ਇੰਕ੍ਰਿਪਟ ਕਰਦਾ ਹੈ ਅਤੇ ਅਣਚਾਹੇ ਵਿਅਕਤੀਆਂ ਤੋਂ ਬਚਾਉਂਦਾ ਹੈ।

How to stay safe on a public, unprotected wifi network

CHEAT SHEET

DO

	Check if the network requires a username and password
	Turn off the option to automatically connect to networks from your device
	Turn off Bluetooth when you're not using it and especially when you're in public places
	Use a secure VPN to ensure your data is encrypted and your device information stays private from snoopers and other bad actors

DON'T

	Use your online banking account or other accounts with crucial sensitive data
	Leave your device unlocked as you step away from it
	Shop online and risk exposing your card information
	Send confidential documents while using a public hotspot and run the risk of exposing their contents to attackers

2. ਪਬਲਿਕ Wi-Fi ਵਰਤਣ ਸਮੇਂ ਸਾਵਧਾਨ ਰਹੋ। ਕਈ ਵਾਰ ਕੈਫੇ, ਏਅਰਪੋਰਟ ਜਾਂ ਹੋਟਲ ਵਿੱਚ ਖੁੱਲ੍ਹਾ Wi-Fi ਹੈ ਜੋ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹੁੰਦਾ। ਇਸ ਤਰ੍ਹਾਂ ਦੇ ਨੈੱਟਵਰਕ 'ਤੇ ਆਪਣੇ ਬੈਂਕ ਜਾਂ ਨਿੱਜੀ ਡਾਟਾ ਨਾਲ ਲੌਗਿਨ ਨਾ ਕਰੋ। ਜੇ ਜ਼ਰੂਰੀ ਹੋਵੇ ਤਾਂ VPN (Virtual Private Network) ਵਰਤੋਂ, ਜੋ ਤੁਹਾਡਾ ਡਾਟਾ ਸੁਰੱਖਿਅਤ ਕਰਦਾ ਹੈ ਅਤੇ ਹੈਕਰ ਤੋਂ ਛੁਪਾ ਰਹਿੰਦਾ ਹੈ।
3. ਆਪਣੇ Wi-Fi ਰਾਊਟਰ ਦੀ ਨਿਯਮਤ ਅਪਡੇਟ ਕਰੋ। ਰਾਊਟਰ ਦੇ ਫਰਮਵੇਅਰ ਨੂੰ ਅਪਡੇਟ ਕਰਨਾ ਸੁਰੱਖਿਆ ਖਤਰੇ ਘਟਾਉਂਦਾ ਹੈ। ਫਾਇਰਵਾਲ ਅਤੇ ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਵੀ ਸੁਰੱਖਿਆ ਵਧਾਉਂਦੇ ਹਨ।
4. Wi-Fi ਨੈਮ (SSID) ਨੂੰ ਪਬਲਿਕ ਨਾ ਕਰੋ। ਆਪਣਾ ਨੈੱਟਵਰਕ “ਹੋਮWiFi” ਜਾਂ ਆਮ ਨਾਂ ਨਾਲ ਨਾ ਛੱਡੋ, ਇਸ ਨਾਲ ਹੈਕਰ ਤੁਹਾਡਾ ਨੈੱਟਵਰਕ ਲੱਭ ਸਕਦੇ ਹਨ।

ਸੰਖੇਪ ਵਿੱਚ, ਸੁਰੱਖਿਅਤ Wi-Fi ਵਰਤੋਂ ਨਾਲ ਨਾ ਸਿਰਫ਼ ਤੁਹਾਡਾ ਡਾਟਾ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦਾ ਹੈ, ਬਲਕਿ ਹੈਕਿੰਗ, ਫਰਾਡ ਅਤੇ ਮਾਲਵੇਅਰ ਤੋਂ ਵੀ ਬਚਾਅ ਹੁੰਦਾ ਹੈ। ਘਰ ਜਾਂ ਪਬਲਿਕ ਨੈੱਟਵਰਕ ਸੁਰੱਖਿਆ ਲਈ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ, ਇੰਕ੍ਰਿਪਸ਼ਨ, VPN, ਨਿਯਮਤ ਅਪਡੇਟ ਅਤੇ ਫਾਇਰਵਾਲ ਵਰਤਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਅਸੀਂ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਤਰੀਕੇ ਨਾਲ ਵਰਤ ਸਕਦੇ ਹਾਂ।

ਪਬਲਿਕ Wi-Fi ਦੇ ਖ਼ਤਰੇ

ਅੱਜਕੱਲ੍ਹ ਪਬਲਿਕ Wi-Fi ਹਰ ਜਗ੍ਹਾ ਉਪਲਬਧ ਹੈ—ਕੈਫੇ, ਏਅਰਪੋਰਟ, ਹੋਟਲ, ਸ਼ਾਪਿੰਗ ਮਾਲ ਅਤੇ ਸਾਰੀਆਂ ਪਬਲਿਕ ਥਾਵਾਂ ‘ਤੇ। ਇਹ ਸੌਖਾ ਅਤੇ ਮੁਫ਼ਤ ਇੰਟਰਨੈੱਟ ਐਕਸੈਸ ਮੁਹੱਈਆ ਕਰਵਾਉਂਦਾ ਹੈ, ਪਰ ਇਸਦੇ ਨਾਲ ਕਈ **ਸਾਈਬਰ ਖ਼ਤਰੇ** ਵੀ ਹਨ। ਸਭ ਤੋਂ ਵੱਡਾ ਖ਼ਤਰਾ ਹੈ **ਹੈਕਿੰਗ**। ਹੈਕਰ ਪਬਲਿਕ Wi-Fi ਨਾਲ ਕਨੈਕਟ ਹੋਏ ਯੂਜ਼ਰਾਂ ਦੇ ਡਿਵਾਈਸਾਂ ਤੱਕ ਅਸਾਨੀ ਨਾਲ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰ ਸਕਦੇ ਹਨ। ਉਹ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਬੈਂਕ ਡਿਟੇਲ, ਪਾਸਵਰਡ ਅਤੇ ਸੰਪਰਕ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ।

ਦੂਜਾ ਖ਼ਤਰਾ ਹੈ **ਮੈਨ-ਇਨ-ਦ-ਮਿਡਲ (MITM) ਅਟੈਕ**। ਇਸ ਤਰ੍ਹਾਂ ਦੇ ਅਟੈਕ ਵਿੱਚ ਹੈਕਰ ਤੁਹਾਡੇ ਅਤੇ ਇੰਟਰਨੈੱਟ ਸਰਵਰ ਦੇ ਵਿਚਕਾਰ ਡਾਟਾ ਰੀਡ ਜਾਂ ਮੋਡੀਫਾਈ ਕਰ ਸਕਦਾ ਹੈ। ਇਸ ਕਾਰਨ, ਤੁਸੀਂ ਜੋ ਵੀ ਡਾਟਾ ਭੇਜ ਰਹੇ ਹੋ—ਜਿਵੇਂ ਲੋਗਿਨ ਡਿਟੇਲ, ਈ-ਮੇਲ ਜਾਂ ਫਾਈਨੈਂਸ਼ਲ ਟ੍ਰਾਂਜੈਕਸ਼ਨ—ਉਹ ਚੋਰੀ ਹੋ ਸਕਦਾ ਹੈ।

ਤੀਜਾ, ਪਬਲਿਕ Wi-Fi ਤੇ **ਮਾਲਵੇਅਰ ਅਤੇ ਵਾਇਰਸ** ਦੇ ਖ਼ਤਰੇ ਵੀ ਵੱਧ ਜਾਂਦੇ ਹਨ। ਹੈਕਰ ਖੁੱਲ੍ਹੇ ਨੈੱਟਵਰਕ ਰਾਹੀਂ ਮਾਲਵੇਅਰ ਫਾਈਲਾਂ ਡਿਵਾਈਸ ‘ਚ ਇੰਸਟਾਲ ਕਰ ਸਕਦਾ ਹੈ, ਜੋ ਡਿਵਾਈਸ ਦੀ ਕਾਰਗੁਜ਼ਾਰੀ ਖ਼ਤਮ ਕਰ ਸਕਦਾ ਹੈ ਅਤੇ ਨਿੱਜੀ ਡਾਟਾ ਚੋਰੀ ਕਰ ਸਕਦਾ ਹੈ।

ਇਸ ਲਈ, ਪਬਲਿਕ Wi-Fi ਵਰਤਣ ਸਮੇਂ **ਸਾਵਧਾਨ ਰਹਿਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ**। ਬੈਕਿੰਗ ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੇ ਲੈਣ-ਦੇਣ ਤੋਂ ਬਚੋ, ਸਿਰਫ਼ HTTPS ਅਤੇ ਭਰੋਸੇਯੋਗ ਸਾਈਟਾਂ ਵਰਤੋਂ, ਅਤੇ ਜਰੂਰੀ ਹੋਣ ‘ਤੇ VPN (Virtual Private Network) ਵਰਤੋਂ। ਨਿਯਮਤ ਤੌਰ ‘ਤੇ ਡਿਵਾਈਸ ਅਪਡੇਟ ਕਰੋ ਅਤੇ ਐਂਟੀਵਾਇਰਸ/ਫਾਇਰਵਾਲ ਸਾਫਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਕਰੋ।

**ਸੰਖੇਪ ਵਿੱਚ, ਪਬਲਿਕ Wi-Fi ਸੁਵਿਧਾ ਦੇ ਨਾਲ ਸਾਈਬਰ ਖ਼ਤਰੇ ਵੀ ਲਿਆਉਂਦਾ ਹੈ।
ਸਾਵਧਾਨੀ ਨਾਲ ਵਰਤੋਂ ਕਰਕੇ ਅਤੇ ਮਜ਼ਬੂਤ ਸੁਰੱਖਿਆ ਉਪਾਅ ਅਪਣਾ ਕੇ ਤੁਸੀਂ ਆਪਣੇ ਡਿਵਾਈਸ
ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹੋ।**

13. ਆਨਲਾਈਨ ਕਲਾਸਾਂ ਅਤੇ ਈ-ਲਰਨਿੰਗ ਸੁਰੱਖਿਆ ਸਬੰਧੀ ਹਦਾਇਤਾਂ

ਆਨਲਾਈਨ ਕਲਾਸਾਂ ਅਤੇ ਈ-ਲਰਨਿੰਗ ਅੱਜ ਦੇ ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਇੱਕ ਮਹੱਤਵਪੂਰਨ ਸਿੱਖਣ ਦਾ ਸਾਧਨ ਬਣ ਗਏ ਹਨ। ਘਰ ਬੈਠੇ ਹੀ ਵਿਦਿਆਰਥੀ ਲਾਈਵ ਕਲਾਸਾਂ, ਵੀਡੀਓ ਲੈਕਚਰ, ਕਵਿਜ਼ ਅਤੇ ਡਿਜ਼ਿਟਲ ਅਸਾਈਨਮੈਂਟ ਕਰ ਸਕਦੇ ਹਨ। ਪਰ ਇਸਨੂੰ ਵਰਤਦਿਆਂ **ਡਿਜ਼ਿਟਲ ਸੁਰੱਖਿਆ** ਦਾ ਧਿਆਨ ਰੱਖਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਕਿਉਂਕਿ ਆਨਲਾਈਨ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ ਕਈ ਵਾਰੀ ਸਾਈਬਰ ਖਤਰੇ ਵੀ ਹੋ ਸਕਦੇ ਹਨ।



ਸਭ ਤੋਂ ਪਹਿਲਾਂ, ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ **ਸੁਰੱਖਿਅਤ ਪਾਸਵਰਡ ਅਤੇ ਯੂਜ਼ਰ ਨੇਮ** ਵਰਤਣਾ ਚਾਹੀਦਾ ਹੈ। ਪਾਸਵਰਡ ਮਜ਼ਬੂਤ, ਯੂਨੀਕ ਅਤੇ ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਅਪਡੇਟ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ। ਆਨਲਾਈਨ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ ਵਿਦਿਆਰਥੀ ਦੀਆਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀਆਂ—ਜਿਵੇਂ ਕਿ ਨਾਮ, ਸਕੂਲ ID, ਈਮੇਲ ਅਤੇ ਅਸਾਈਨਮੈਂਟ—ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਇਹ ਮਹੱਤਵਪੂਰਨ ਹੈ।

ਦੂਜਾ, **ਵੈਬਕੈਮ ਅਤੇ ਮਾਈਕ੍ਰੋਫੋਨ ਸੁਰੱਖਿਆ** ਵੀ ਜ਼ਰੂਰੀ ਹੈ। ਕਈ ਵਾਰੀ ਹੈਕਰ ਵੈਬਕੈਮ ਰਾਹੀਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਲਈ ਜਦੋਂ ਵਰਤੋਂ ਨਾ ਹੋਵੇ, ਤਦੋਂ ਮਾਈਕ੍ਰੋਫੋਨ ਅਤੇ ਵੈਬਕੈਮ ਨੂੰ ਬੰਦ ਰੱਖੇ ਜਾਂ ਕਵਰ ਕਰੇ।

ਤੀਜਾ, ਆਨਲਾਈਨ ਪਲੇਟਫਾਰਮਾਂ 'ਤੇ **ਨਾਜਾਇਜ਼ ਲਿੰਕਾਂ ਅਤੇ ਫਾਇਲਾਂ** 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ। ਕੁਝ ਫਰਾਡ ਈਮੇਲ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪੋਸਟਾਂ ਰਾਹੀਂ ਮਾਲਵੇਅਰ ਜਾਂ ਵਾਇਰਸ ਡਿਵਾਈਸ ਵਿੱਚ ਇੰਸਟਾਲ ਹੋ ਸਕਦਾ ਹੈ। ਇਸ ਲਈ ਸਿਰਫ ਭਰੋਸੇਯੋਗ ਸਰੋਤਾਂ ਤੋਂ ਹੀ ਡਾਊਨਲੋਡ ਅਤੇ ਲਿੰਕ ਖੋਲ੍ਹੋ।

ਚੋਥਾ, ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਸਿੱਖਾਇਆ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ **ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਚੈਟ ਨਾ ਕਰਨ** ਅਤੇ ਕਲਾਸਾਂ ਦਾ ਪਾਸਵਰਡ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰਨ। ਇਹ ਹੇਠਾਂ ਦਿੱਤੇ ਗਏ ਨੈਟਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਦੇ ਨਿਯਮਾਂ ਨਾਲ ਸੁਰੱਖਿਆ ਨੂੰ ਬਹਾਲ ਰੱਖਦਾ ਹੈ।

ਸੁਰੱਖਿਅਤ ਲਾਗਇੰਨ

ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਲਾਗਇੰਨ ਕਰਨਾ ਹਰ ਆਨਲਾਈਨ ਸਰਵਿਸ ਦੀ ਮੁੱਖ ਸ਼ੁਰੂਆਤ ਹੈ। ਚਾਹੇ ਉਹ ਈ-ਮੇਲ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਬੈਂਕਿੰਗ ਐਪ, ਆਨਲਾਈਨ ਸਟੱਡੀ ਪੋਰਟਲ ਜਾਂ ਗੇਮਿੰਗ ਪਲੇਟਫਾਰਮ ਹੋਵੇ, **ਸੁਰੱਖਿਅਤ ਲਾਗਇੰਨ** ਤੁਹਾਡੇ ਡਾਟਾ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ ਲਈ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਸਭ ਤੋਂ ਪਹਿਲਾਂ, **ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ** ਵਰਤਣਾ ਅਤਿ ਜ਼ਰੂਰੀ ਹੈ। ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਵਿੱਚ ਵੱਡੇ ਅਤੇ ਛੋਟੇ ਅੱਖਰ, ਅੰਕ ਅਤੇ ਵਿਸ਼ੇਸ਼ ਚਿੰਨ੍ਹ ਸ਼ਾਮਲ ਹੋਣੇ ਚਾਹੀਦੇ ਹਨ। ਇੱਕੋ ਜਿਹਾ ਪਾਸਵਰਡ ਕਈ ਖਾਤਿਆਂ ਲਈ ਵਰਤੋਂ ਨਾ ਕਰੋ। ਇਹ ਹੈਕਰਾਂ ਤੋਂ ਤੁਹਾਡਾ ਖਾਤਾ ਹੈਕ ਹੋਣ ਤੋਂ ਬਚਾਉਂਦਾ ਹੈ।

ਦੂਜਾ, **Two-Factor Authentication (2FA)** ਵਰਤੋਂ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਸ ਤਰੀਕੇ ਨਾਲ, ਲਾਗਇੰਨ ਕਰਨ ਲਈ ਸਿਰਫ਼ ਪਾਸਵਰਡ ਹੀ ਨਹੀਂ, ਸੈਕੰਡਰੀ ਕੋਡ ਜਾਂ OTP (One-Time Password) ਵੀ ਲੋੜੀਂਦਾ ਹੁੰਦਾ ਹੈ। ਇਸ ਨਾਲ, ਜੇ ਪਾਸਵਰਡ ਚੋਰੀ ਵੀ ਹੋ ਜਾਵੇ, ਤਾਂ ਵੀ ਖਾਤਾ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦਾ ਹੈ।

ਤੀਜਾ, ਲਾਗਇੰਨ ਕਰਨ ਸਮੇਂ **ਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕ** ਵਰਤੋਂ। ਪਬਲਿਕ Wi-Fi ਤੇ ਲਾਗਇੰਨ ਕਰਨਾ ਸੁਰੱਖਿਆ ਖ਼ਤਰੇ ਵਧਾ ਸਕਦਾ ਹੈ। VPN (Virtual Private Network) ਵਰਤਣਾ ਇਸ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਉਂਦਾ ਹੈ।

ਚੋਥਾ, **ਆਪਣੇ ਖਾਤਿਆਂ ਦੀ ਨਿਯਮਤ ਜਾਂਚ** ਕਰੋ। ਅਣਜਾਣ ਲਾਗਇੰਨ ਐਕਟਿਵਿਟੀ ਦੇਖੋ ਅਤੇ ਜੇ ਕੋਈ ਸ਼ੱਕੀ ਕਿਰਿਆ ਮਿਲੇ, ਤਾਂ ਤੁਰੰਤ ਪਾਸਵਰਡ ਬਦਲੋ।

ਸੰਖੇਪ ਵਿੱਚ, ਸੁਰੱਖਿਅਤ ਲਾਗਇਨ ਲਈ **ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ, 2FA, ਸੁਰੱਖਿਅਤ ਨੈੱਟਵਰਕ ਅਤੇ ਨਿਯਮਤ ਨਿਗਰਾਨੀ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹਨ। ਇਹ ਉਪਾਅ ਅਪਣਾਉਣ ਨਾਲ ਤੁਸੀਂ ਆਪਣੇ ਡਿਜ਼ਿਟਲ ਖਾਤਿਆਂ ਨੂੰ ਹੈਕਿੰਗ, ਫਰਾਡ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਤੋਂ ਬਚਾ ਸਕਦੇ ਹੋ।

ਅਧਿਆਪਕਾਂ ਨਾਲ ਸਾਂਝਾ ਕਰਨ ਵਾਲੀ ਜਾਣਕਾਰੀ ਦੀ ਸੀਮਾ

ਆਨਲਾਈਨ ਅਤੇ ਸਕੂਲ ਸੈਟਿੰਗ ਵਿੱਚ ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਅਧਿਆਪਕਾਂ ਨਾਲ ਜਾਣਕਾਰੀ ਸਾਂਝਾ ਕਰਨਾ ਆਮ ਹੈ। ਇਸ ਨਾਲ ਸਿੱਖਣ ਦੀ ਪ੍ਰਕਿਰਿਆ ਸੁਚਾਰੂ ਬਣਦੀ ਹੈ ਅਤੇ ਵਿਦਿਆਰਥੀ ਨੂੰ ਸਹਾਇਤਾ ਮਿਲਦੀ ਹੈ। ਪਰ ਇਹ ਵੀ ਜ਼ਰੂਰੀ ਹੈ ਕਿ ਵਿਦਿਆਰਥੀ **ਜਾਣਕਾਰੀ ਦੀ ਸੀਮਾ** ਸਮਝਣ ਅਤੇ ਉਸਦਾ ਪਾਲਣ ਕਰਨ।

ਸਭ ਤੋਂ ਪਹਿਲਾਂ, ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਸਿਰਫ **ਅਧਿਆਪਕਾਂ ਲਈ ਲੋੜੀਂਦੀ ਜਾਣਕਾਰੀ** ਹੀ ਸਾਂਝੀ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। ਜਿਵੇਂ ਕਿ ਰਜਿਸਟ੍ਰੇਸ਼ਨ ਡੀਟੇਲ, ਸਕੂਲ ID, ਅਸਾਈਨਮੈਂਟ, ਪ੍ਰਗਤੀ ਰਿਪੋਰਟ ਅਤੇ ਅਟੈਂਡੈਂਸ। ਇਹ ਜਾਣਕਾਰੀ ਅਧਿਆਪਕਾਂ ਨੂੰ ਵਿਦਿਆਰਥੀ ਦੀ ਪੜ੍ਹਾਈ ਅਤੇ ਸਹਾਇਤਾ ਲਈ ਲੋੜੀਂਦੀ ਹੈ।

ਦੂਜਾ, ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ **ਨਿੱਜੀ ਜਾਣਕਾਰੀ** ਜਿਵੇਂ ਪਾਸਵਰਡ, ਬੈਂਕ ਡੀਟੇਲ, OTP, ਆਧਾਰ ਨੰਬਰ ਜਾਂ ਫੋਨ ਪਿੰਨ ਕੋਡ ਸਾਂਝਾ ਨਹੀਂ ਕਰਨੇ ਚਾਹੀਦੇ। ਇਹ ਜਾਣਕਾਰੀ ਅਧਿਆਪਕਾਂ ਨਾਲ ਸਾਂਝਾ ਕਰਨ ਦੀ ਲੋੜ ਨਹੀਂ ਹੁੰਦੀ ਅਤੇ ਇਸਨੂੰ ਸਾਂਝਾ ਕਰਨ ਨਾਲ ਸੁਰੱਖਿਆ ਖ਼ਤਰੇ ਵੱਧ ਜਾਂਦੇ ਹਨ।

ਤੀਜਾ, ਆਨਲਾਈਨ ਕਲਾਸਾਂ ਜਾਂ ਗੇਮਿੰਗ ਪਲੇਟਫਾਰਮਾਂ ਤੇ ਵੀ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਸਿਰਫ਼ ਲਾਜ਼ਮੀ ਡੀਟੇਲ ਦੇਣੇ ਚਾਹੀਦੇ ਹਨ। ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਲਿੰਕ ਜਾਂ ਫਾਈਲ ਸਾਂਝੀ ਨਾ ਕਰੋ। ਇਹ ਹੇਠਾਂ ਦਿੱਤੇ ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਦੇ ਨਿਯਮਾਂ ਨਾਲ ਸੁਰੱਖਿਆ ਨੂੰ ਬਹਾਲ ਰੱਖਦਾ ਹੈ।

ਸੰਖੇਪ ਵਿੱਚ, ਅਧਿਆਪਕਾਂ ਨਾਲ ਸਾਂਝਾ ਕਰਨ ਵਾਲੀ ਜਾਣਕਾਰੀ ਦੀ ਸੀਮਾ ਨੂੰ ਸਮਝਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਸਿਰਫ਼ ਲੋੜੀਂਦੀ ਅਤੇ ਸੁਰੱਖਿਅਤ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਨਾਲ ਵਿਦਿਆਰਥੀ ਆਪਣੀ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਬਰਕਰਾਰ ਰੱਖ ਸਕਦੇ ਹਨ ਅਤੇ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂ ਸੁਰੱਖਿਅਤ ਬਣਦੀ ਹੈ।

Online Meeting links ਦੀ ਸੁਰੱਖਿਆ

ਆਨਲਾਈਨ ਕਲਾਸਾਂ, ਵਿਡੀਓ ਕਾਨਫਰੰਸ ਅਤੇ ਵਿਰਚੁਅਲ ਮੀਟਿੰਗਾਂ ਅੱਜਕੱਲ੍ਹ ਸਿੱਖਣ ਅਤੇ ਕਾਰੋਬਾਰ ਦਾ ਅਤਿ ਜ਼ਰੂਰੀ ਹਨ। ਪਰ, ਜੇ ਮੀਟਿੰਗ ਲਿੰਕ ਸੁਰੱਖਿਅਤ ਨਾ ਹੋਵੇ, ਤਾਂ ਹੈਕਰ ਜਾਂ ਅਣਜਾਣ ਵਿਅਕਤੀ ਅਸਾਨੀ ਨਾਲ ਲਿੰਕ ਰਾਹੀਂ ਮੀਟਿੰਗ ਵਿੱਚ ਦਾਖਲ ਹੋ ਸਕਦੇ ਹਨ। ਇਸ ਲਈ **Meeting Links ਦੀ ਸੁਰੱਖਿਆ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

1. ਮੀਟਿੰਗ ਲਿੰਕ **ਭਰੋਸੇਮੰਦ ਸਰੋਤਾਂ ਤੋਂ ਹੀ ਸਾਂਝਾ ਕਰੋ**। ਕਦੇ ਵੀ ਲਿੰਕ ਨੂੰ ਸੋਸ਼ਲ ਮੀਡੀਆ, ਅਣਜਾਣ ਈਮੇਲ ਜਾਂ ਪਬਲਿਕ ਫੋਰਮ 'ਤੇ ਪੇਸਟ ਨਾ ਕਰੋ। ਇਸ ਨਾਲ "Zoombombing" ਜਾਂ ਹੈਕਿੰਗ ਦੇ ਖਤਰੇ ਘਟ ਜਾਂਦੇ ਹਨ।
2. ਮੀਟਿੰਗ ਲਈ **ਪਾਸਵਰਡ ਅਤੇ ਲਾਕ ਫੀਚਰ** ਵਰਤੋਂ। ਜੇ ਮੀਟਿੰਗ ਪਾਸਵਰਡ ਸੈੱਟ ਹੋਵੇ, ਤਾਂ ਕੇਵਲ ਭਰੋਸੇਮੰਦ ਵਿਅਕਤੀਆਂ ਨੂੰ ਪਾਸਵਰਡ ਦਿੱਤਾ ਜਾ ਸਕਦਾ ਹੈ। ਮੀਟਿੰਗ ਸ਼ੁਰੂ ਹੋਣ ਤੋਂ ਬਾਅਦ ਲਾਕ ਫੀਚਰ ਚਾਲੂ ਕਰਨਾ ਵੀ ਸੁਰੱਖਿਆ ਵਧਾਉਂਦਾ ਹੈ।
3. **ਵੇਟਿੰਗ ਰੂਮ (Waiting Room) ਫੀਚਰ** ਵਰਤੋਂ। ਇਸ ਨਾਲ ਮੀਟਿੰਗ ਦੇ ਹੋਸਟ ਨੂੰ ਪਤਾ ਰਹਿੰਦਾ ਹੈ ਕਿ ਕੋਣ-ਕੋਣ ਆ ਰਹੇ ਹਨ ਅਤੇ ਕੋਈ ਅਣਜਾਣ ਵਿਅਕਤੀ ਮੀਟਿੰਗ ਵਿੱਚ ਦਾਖਲ ਨਾ ਹੋਵੇ।
4. ਮੀਟਿੰਗ ਦੌਰਾਨ **ਸਹਾਇਤਾ ਸਦੱਸਾਂ ਦੀ ਨਿਗਰਾਨੀ** ਕਰੋ। ਅਣਜਾਣ ਯੂਜ਼ਰਾਂ ਨੂੰ ਸੱਦਾ ਨਾ ਦਿਓ ਅਤੇ ਸਿਖਿਆਰਥੀਆਂ ਨੂੰ ਸਿਖਾਓ ਕਿ ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨ।

ਸੰਖੇਪ ਵਿੱਚ, Meeting Links ਦੀ ਸੁਰੱਖਿਆ ਲਈ **ਭਰੋਸੇਮੰਦ ਸਾਂਝਾ, ਪਾਸਵਰਡ, ਲਾਕ ਅਤੇ ਵੇਟਿੰਗ ਰੂਮ ਫੀਚਰ, ਅਤੇ ਨਿਗਰਾਨੀ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹਨ। ਇਹ ਉਪਾਅਵਾਂ ਮੀਟਿੰਗਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਅਤੇ ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਨਿਰਭਰਯੋਗ ਬਣਾਉਂਦੇ ਹਨ।

14. ਆਨਲਾਈਨ ਸਿੱਖਣ ਅਤੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਸਬੰਧੀ ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਦੀ ਭੂਮਿਕਾ

ਆਨਲਾਈਨ ਸਿੱਖਣ ਅਤੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਅਤੇ ਸਿੱਖਣ ਦੇ ਮਿਆਰ ਨੂੰ ਯਕੀਨੀ ਬਣਾਉਣ ਵਿੱਚ ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਦੀ ਭੂਮਿਕਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਹ ਭੂਮਿਕਾ ਸਿਰਫ ਨਿਗਰਾਨੀ ਤੱਕ ਸੀਮਤ ਨਹੀਂ, ਬਲਕਿ ਸਿੱਖਣ, ਸਮਝਾਉਣ ਅਤੇ ਸੁਰੱਖਿਅਤ ਆਨਲਾਈਨ ਵਰਤੋਂ ਦੀ ਸਿੱਖਿਆ ਦੇਣ ਤੱਕ ਵੀ ਹੈ।

ਸਭ ਤੋਂ ਪਹਿਲਾਂ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਆਨਲਾਈਨ ਵਰਤੋਂ ਦੇ ਨਿਯਮ ਸਿੱਖਾਉਣੇ ਚਾਹੀਦੇ ਹਨ। ਇਸ ਵਿੱਚ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝਾ ਕਰਨ ਦੀ ਸੀਮਾ, ਪਾਸਵਰਡ ਸੁਰੱਖਿਆ, ਅਣਜਾਣ ਲਿੰਕਾਂ ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨਾ, ਅਤੇ ਸੁਰੱਖਿਅਤ Wi-Fi ਵਰਤਣਾ ਸ਼ਾਮਲ ਹੈ। ਬੱਚਿਆਂ ਨੂੰ ਸਮਝਾਉਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਕਿਸੇ ਵੀ ਈਮੇਲ, ਮੈਸੇਜ ਜਾਂ ਐਪ ਦੇ ਸਬੂਤ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚਣਾ ਕਿੰਨਾ ਜ਼ਰੂਰੀ ਹੈ।



ਦੂਜਾ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਬੱਚਿਆਂ ਦੀ ਨਿਗਰਾਨੀ ਕਰਨ ਦੀ ਲੋੜ ਹੈ। ਘਰ ਵਿੱਚ ਮਾਪੇ ਸਕੂਲ ਦੀਆਂ ਆਨਲਾਈਨ ਕਲਾਸਾਂ, ਡਿਜ਼ਿਟਲ ਅਸਾਈਨਮੈਂਟ ਅਤੇ ਮੋਬਾਈਲ ਐਕਟਿਵਿਟੀ 'ਤੇ ਨਜ਼ਰ ਰੱਖ ਸਕਦੇ ਹਨ। ਅਧਿਆਪਕਾਂ ਲਈ ਵੀ ਇਹ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਉਹ ਵਿਦਿਆਰਥੀਆਂ ਦੀਆਂ ਆਨਲਾਈਨ ਕਲਾਸਾਂ ਅਤੇ ਸਮੱਗਰੀ ਦੀ ਸੁਰੱਖਿਆ ਯਕੀਨੀ

ਬਣਾਏ। ਇਹ ਨਿਗਰਾਨੀ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਅਤੇ ਖਤਰਨਾਕ ਵੈਬਸਾਈਟਾਂ ਜਾਂ ਫਰਾਡੀ ਲਿੰਕਾਂ ਤੋਂ ਬਚਾਉਂਦੀ ਹੈ।

ਤੀਜਾ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਬੱਚਿਆਂ ਨੂੰ **ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ** ਦੇਣੀ ਚਾਹੀਦੀ ਹੈ। ਇਸ ਵਿੱਚ ਫਿਸ਼ਿੰਗ, OTP ਫਰਾਡ, ਨਕਲੀ ਖਬਰਾਂ, ਮਾਲਵੇਅਰ ਅਤੇ ਹੈਕਿੰਗ ਵਰਗੇ ਖਤਰਿਆਂ ਬਾਰੇ ਜਾਣਕਾਰੀ ਸ਼ਾਮਲ ਹੈ। ਜਦੋਂ ਬੱਚੇ ਇਹਨਾਂ ਖਤਰਿਆਂ ਨੂੰ ਸਮਝਦੇ ਹਨ, ਤਾਂ ਉਹ ਸੁਚੇਤ ਅਤੇ ਨਿਰਭਰਯੋਗ ਤਰੀਕੇ ਨਾਲ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਰਤ ਸਕਦੇ ਹਨ।

ਚੌਥਾ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਬੱਚਿਆਂ ਨੂੰ **ਸੁਰੱਖਿਅਤ ਆਨਲਾਈਨ ਆਦਤਾਂ ਅਤੇ ਡਿਜ਼ਿਟਲ ਐਟਿਕੇਟ** ਸਿਖਾਉਣੇ ਚਾਹੀਦੇ ਹਨ। ਇਸ ਵਿੱਚ ਹੋਰਨਾਂ ਦੀ ਇੱਜ਼ਤ, ਆਨਲਾਈਨ ਵਿਹਾਰ ਦੇ ਨਿਯਮ ਅਤੇ ਨੈਤਿਕ ਵਰਤੋਂ ਸ਼ਾਮਲ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਬੱਚੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆਂ ਵਿੱਚ ਸੁਰੱਖਿਅਤ, ਜ਼ਿੰਮੇਵਾਰ ਅਤੇ ਨੈਤਿਕ ਤਰੀਕੇ ਨਾਲ ਹਿੱਸਾ ਲੈ ਸਕਦੇ ਹਨ।

ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਦੀ ਭੂਮਿਕਾ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਅਤੇ ਨਿਰਭਰਯੋਗ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂ ਦੀ ਸਿੱਖਿਆ ਦੇਣ, ਨਿਗਰਾਨੀ ਕਰਨ, ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ ਦੇਣ ਅਤੇ ਡਿਜ਼ਿਟਲ ਆਦਤਾਂ ਦਾ ਸਹੀ ਰਸਤਾ ਦਿਖਾਉਣ ਤੱਕ ਸੀਮਿਤ ਹੈ। ਇਹ ਭੂਮਿਕਾ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਸਮਰਥ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂਕਾਰ ਬਣਾਉਂਦੀ ਹੈ, ਜੋ ਆਨਲਾਈਨ ਦੁਨੀਆ ਦੇ ਖਤਰੇ ਤੋਂ ਬਚਦੇ ਹਨ ਅਤੇ ਸੁਚੇਤ ਰਹਿ ਕੇ ਸਿੱਖਣ ਦਾ ਲੁਤਫ਼ ਲੈਂਦੇ ਹਨ।

ਬੱਚਿਆਂ ਦੀ ਆਨਲਾਈਨ ਐਕਟਿਵਿਟੀ ਦੀ ਮਾਨੀਟਰਿੰਗ

ਅੱਜਕੱਲ੍ਹ ਬੱਚੇ ਘਰ 'ਚ ਵੱਡੇ ਪੈਮਾਨੇ 'ਤੇ ਇੰਟਰਨੈੱਟ ਅਤੇ ਡਿਜ਼ਿਟਲ ਡਿਵਾਈਸ ਵਰਤ ਰਹੇ ਹਨ। ਆਨਲਾਈਨ ਕਲਾਸਾਂ, ਈ-ਲਰਨਿੰਗ ਪੋਰਟਲ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਗੇਮਿੰਗ ਅਤੇ ਮਨੋਰੰਜਨ ਦੀ ਵਰਤੋਂ ਬੱਚਿਆਂ ਲਈ ਸਿੱਖਣ ਅਤੇ ਮਨੋਰੰਜਨ ਦਾ ਸਾਧਨ ਹੈ। ਪਰ, ਇਸ ਨਾਲ ਸਾਈਬਰ ਖਤਰੇ ਅਤੇ ਅਣਜਾਣ ਸੰਪਰਕ ਦੇ ਖਤਰੇ ਵੀ ਵੱਧ ਜਾਂਦੇ ਹਨ। ਇਸ ਲਈ **ਬੱਚਿਆਂ ਦੀ ਆਨਲਾਈਨ ਐਕਟਿਵਿਟੀ ਦੀ ਮਾਨੀਟਰਿੰਗ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਸਭ ਤੋਂ ਪਹਿਲਾਂ, ਮਾਪਿਆਂ ਨੂੰ ਬੱਚਿਆਂ ਦੇ ਡਿਵਾਈਸ ਦੀ ਵਰਤੋਂ 'ਤੇ ਨਿਗਰਾਨੀ ਰੱਖਣੀ ਚਾਹੀਦੀ ਹੈ। ਇਹ ਮਾਨੀਟਰਿੰਗ ਸਿਰਫ਼ ਬੱਚੇ ਨੂੰ ਸਖ਼ਤ ਰੋਕਣ ਲਈ ਨਹੀਂ, ਬਲਕਿ ਉਨ੍ਹਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਆਨਲਾਈਨ ਵਰਤੋਂ

ਸਿੱਖਾਉਣ ਲਈ ਹੈ। ਮਾਪੇ ਵੇਖ ਸਕਦੇ ਹਨ ਕਿ ਬੱਚੇ ਕਿਹੜੀਆਂ ਵੈਬਸਾਈਟਾਂ ਤੇ ਜਾ ਰਹੇ ਹਨ, ਕਿਹੜੇ ਐਪਸ ਵਰਤ ਰਹੇ ਹਨ ਅਤੇ ਕਿਸ ਤਰ੍ਹਾਂ ਦੀ ਸਮੱਗਰੀ ਉਨ੍ਹਾਂ ਨਾਲ ਸੰਪਰਕ ਕਰ ਰਹੀ ਹੈ।

ਦੂਜਾ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਬੱਚਿਆਂ ਨਾਲ ਖੁੱਲ੍ਹ ਕੇ ਚਰਚਾ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ। ਬੱਚਿਆਂ ਨੂੰ ਸਮਝਾਉਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਕਿਹੜੇ ਖ਼ਤਰੇ ਆਨਲਾਈਨ ਹਨ, ਜਿਵੇਂ ਕਿ ਫਿਸ਼ਿੰਗ, OTP ਫਰਾਡ, ਨਕਲੀ ਖਬਰਾਂ ਅਤੇ ਮਾਲਵੇਅਰ। ਇਹ ਚਰਚਾ ਬੱਚਿਆਂ ਨੂੰ ਜਾਗਰੂਕ ਕਰਦੀ ਹੈ ਅਤੇ ਉਹ ਸੁਰੱਖਿਅਤ ਫੈਸਲੇ ਲੈ ਸਕਦੇ ਹਨ।

ਤੀਜਾ, ਮਾਪਿਆਂ ਲਈ **ਪੇਰੈਂਟਲ ਕੰਟਰੋਲ ਸਾਫਟਵੇਅਰ ਅਤੇ ਐਪਸ** ਦੀ ਵਰਤੋਂ ਬਹੁਤ ਮਦਦਗਾਰ ਹੈ। ਇਹ ਸਾਫਟਵੇਅਰ ਬੱਚਿਆਂ ਦੀ ਐਕਟਿਵਿਟੀ ਨੂੰ ਟ੍ਰੈਕ ਕਰਦੇ ਹਨ, ਅਣਚਾਹੇ ਵੈਬਸਾਈਟਾਂ ਨੂੰ ਬਲੌਕ ਕਰਦੇ ਹਨ ਅਤੇ ਸਕ੍ਰੀਨ ਟਾਈਮ ਸੀਮਾ ਨਿਰਧਾਰਤ ਕਰਦੇ ਹਨ। ਇਸ ਨਾਲ ਬੱਚੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆਂ ਦਾ ਸੁਰੱਖਿਅਤ ਤਰੀਕੇ ਨਾਲ ਵਰਤੋਂ ਕਰਦੇ ਹਨ।

ਚੌਥਾ, ਬੱਚਿਆਂ ਦੀ ਆਨਲਾਈਨ ਐਕਟਿਵਿਟੀ ਦੀ ਮਾਨੀਟਰਿੰਗ ਨਾਲ ਬੱਚੇ ਨਾ ਸਿਰਫ਼ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦੇ ਹਨ, ਬਲਕਿ ਉਨ੍ਹਾਂ ਵਿੱਚ **ਨੈਤਿਕ ਆਨਲਾਈਨ ਵਰਤੋਂ ਅਤੇ ਡਿਜ਼ਿਟਲ ਜ਼ਿੰਮੇਵਾਰੀ** ਵੀ ਵਿਕਸਿਤ ਹੁੰਦੀ ਹੈ। ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਦੀ ਨਿਗਰਾਨੀ ਅਤੇ ਸਹਾਇਤਾ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਸਮਰਥ ਅਤੇ ਸੂਝਵਾਨ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂਕਾਰ ਬਣਾਉਂਦੀ ਹੈ।

ਸੰਖੇਪ ਵਿੱਚ, ਬੱਚਿਆਂ ਦੀ ਆਨਲਾਈਨ ਐਕਟਿਵਿਟੀ ਦੀ ਮਾਨੀਟਰਿੰਗ ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਲਈ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਨਿਗਰਾਨੀ, ਖੁੱਲ੍ਹੀ ਚਰਚਾ, ਪੇਰੈਂਟਲ ਕੰਟਰੋਲ ਅਤੇ ਸੁਰੱਖਿਅਤ ਆਦਤਾਂ ਬੱਚਿਆਂ ਨੂੰ ਸਾਈਬਰ ਖ਼ਤਰੇ ਤੋਂ ਬਚਾਉਂਦੇ ਹਨ ਅਤੇ ਉਨ੍ਹਾਂ ਦਾ ਡਿਜ਼ਿਟਲ ਸਿੱਖਣ ਅਨੁਭਵ ਸੁਰੱਖਿਅਤ ਅਤੇ ਨਿਰਭਰਯੋਗ ਬਣਾਉਂਦੇ ਹਨ।

ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ

ਅੱਜਕੱਲ੍ਹ ਡਿਜ਼ਿਟਲ ਯੁੱਗ ਵਿੱਚ ਬੱਚੇ ਘਰ ਬੈਠੇ ਵੀ ਇੰਟਰਨੈੱਟ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਆਨਲਾਈਨ ਪਲੇਟਫਾਰਮ ਵਰਤ ਰਹੇ ਹਨ। ਇਸ ਦੌਰਾਨ, ਮਾਪਿਆਂ ਅਤੇ ਬੱਚਿਆਂ ਵਿਚਕਾਰ **ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ, ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਬੱਚੇ ਆਪਣੇ ਸਵਾਲ, ਚਿੰਤਾਵਾਂ ਅਤੇ ਆਨਲਾਈਨ ਅਨੁਭਵ ਬਾਰੇ ਖੁੱਲ੍ਹ ਕੇ ਗੱਲ ਕਰ ਸਕਦੇ ਹਨ।

ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ ਮਾਪਿਆਂ ਨੂੰ ਬੱਚਿਆਂ ਦੀਆਂ ਆਨਲਾਈਨ ਐਕਟਿਵਿਟੀ, ਦੇਸਤਾਂ, ਮਨੋਰੰਜਨ ਅਤੇ ਸਿੱਖਣ ਦੇ ਤਰੀਕਿਆਂ ਨੂੰ ਸਮਝਣ ਵਿੱਚ ਮਦਦ ਕਰਦਾ ਹੈ। ਜਦੋਂ ਬੱਚੇ ਆਪਣੇ ਮਾਪਿਆਂ ਨਾਲ ਆਨਲਾਈਨ ਅਨੁਭਵ ਸਾਂਝੇ ਕਰਦੇ ਹਨ, ਉਹ ਸੁਰੱਖਿਆ ਨਾਲ ਜੁੜੇ ਖਤਰੇ, ਜਿਵੇਂ ਕਿ ਫਿਸ਼ਿੰਗ, ਨਕਲੀ ਖਬਰਾਂ ਜਾਂ ਪਬਲਿਕ Wi-Fi ਖਤਰੇ ਬਾਰੇ ਵੀ ਖੁੱਲ੍ਹ ਕੇ ਗੱਲ ਕਰ ਸਕਦੇ ਹਨ।

ਇਸ ਸੰਚਾਰ ਦਾ ਇੱਕ ਮਹੱਤਵਪੂਰਨ ਹਿੱਸਾ ਇਹ ਹੈ ਕਿ ਬੱਚੇ ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਵਿਅਕਤੀ ਜਾਂ ਸ਼ੱਕੀ ਲਿੰਕ ਦੇ ਸੰਪਰਕ ਵਿੱਚ ਆਉਣ ਤੇ ਮਾਪਿਆਂ ਤੋਂ ਸਹਾਇਤਾ ਲੈ ਸਕਣ। ਜੇ ਬੱਚੇ ਖੁੱਲ੍ਹ ਕੇ ਗੱਲ ਕਰਦੇ ਹਨ, ਤਾਂ ਮਾਪੇ ਸਮਝਦਾਰੀ ਨਾਲ ਰਾਹ ਦਿਖਾ ਸਕਦੇ ਹਨ ਅਤੇ ਬੱਚੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਫੈਸਲੇ ਲੈਣਾ ਸਿਖਾ ਸਕਦੇ ਹਨ।

ਮਾਪਿਆਂ ਲਈ ਵੀ ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ ਇਹ ਯਕੀਨੀ ਬਣਾਉਂਦਾ ਹੈ ਕਿ ਉਹ ਬੱਚਿਆਂ ਦੀਆਂ ਆਨਲਾਈਨ ਆਦਤਾਂ, ਸਕੂਲ ਅਸਾਈਨਮੈਂਟ ਅਤੇ ਮਨੋਰੰਜਨ ਦੀ ਸਮਝ ਰੱਖ ਸਕਣ। ਇਹ ਸੰਚਾਰ ਬੱਚਿਆਂ ਵਿੱਚ ਭਰੋਸਾ ਅਤੇ ਸੁਰੱਖਿਆ ਦੀ ਭਾਵਨਾ ਪੈਦਾ ਕਰਦਾ ਹੈ।

ਸੰਖੇਪ ਵਿੱਚ, **ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ** ਮਾਪਿਆਂ ਅਤੇ ਬੱਚਿਆਂ ਵਿਚਕਾਰ ਭਰੋਸਾ ਬਣਾਉਂਦਾ ਹੈ, ਬੱਚਿਆਂ ਨੂੰ ਆਨਲਾਈਨ ਖਤਰੇ ਤੋਂ ਸੁਰੱਖਿਅਤ ਰੱਖਦਾ ਹੈ ਅਤੇ ਉਨ੍ਹਾਂ ਨੂੰ ਜ਼ਿੰਮੇਵਾਰ ਅਤੇ ਨੈਤਿਕ ਤਰੀਕੇ ਨਾਲ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਰਤਣ ਸਿਖਾਉਂਦਾ ਹੈ। ਇਹ ਸੰਚਾਰ ਸਿਰਫ਼ ਸੁਰੱਖਿਆ ਹੀ ਨਹੀਂ, ਬਲਕਿ ਬੱਚਿਆਂ ਦੇ ਆਤਮ-ਵਿਕਾਸ ਅਤੇ ਸਿੱਖਣ ਦੀ ਪ੍ਰਕਿਰਿਆ ਲਈ ਵੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਸਾਂਝੀ ਜ਼ਿੰਮੇਵਾਰੀ

ਅੱਜਕੱਲ੍ਹ ਦੀ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਅਤੇ ਸਿੱਖਣ ਲਈ **ਮਾਪਿਆਂ ਅਤੇ ਬੱਚਿਆਂ ਵਿਚਕਾਰ ਸਾਂਝੀ ਜ਼ਿੰਮੇਵਾਰੀ** ਬਹੁਤ ਅਹੰਸਭਾਗ ਹੈ। ਇਸ ਦਾ ਮਤਲਬ ਹੈ ਕਿ ਮਾਪੇ ਅਤੇ ਬੱਚੇ ਮਿਲ ਕੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਨੈਤਿਕ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਤਰੀਕੇ ਨਾਲ ਵਰਤਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨ।

ਮਾਪਿਆਂ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਇਹ ਹੈ ਕਿ ਉਹ ਬੱਚਿਆਂ ਨੂੰ ਆਨਲਾਈਨ ਖਤਰੇ ਬਾਰੇ ਜਾਣੂ ਕਰਵਾਏ। ਇਸ ਵਿੱਚ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ, ਪਾਸਵਰਡ ਸੁਰੱਖਿਆ, ਸੁਰੱਖਿਅਤ Wi-Fi ਵਰਤਣਾ, ਫਿਸ਼ਿੰਗ ਅਤੇ ਮਾਲਵੇਅਰ ਤੋਂ ਬਚਾਅ

ਸਿੱਖਾਉਣਾ ਸ਼ਾਮਲ ਹੈ। ਮਾਪੇ ਬੱਚਿਆਂ ਦੀ ਨਿਗਰਾਨੀ ਕਰਕੇ ਇਹ ਯਕੀਨੀ ਬਣਾਉਂਦੇ ਹਨ ਕਿ ਉਹ ਅਣਜਾਣ ਵੈਬਸਾਈਟਾਂ ਜਾਂ ਲਿੰਕਾਂ ਤੋਂ ਦੂਰ ਰਹਿਣ।

ਬੱਚਿਆਂ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਹੈ ਕਿ ਉਹ ਮਾਪਿਆਂ ਦੀ ਸਲਾਹ ਮੰਨਣ ਅਤੇ ਸੁਰੱਖਿਆ ਨਿਯਮਾਂ ਦੀ ਪਾਲਣਾ ਕਰਨ। ਬੱਚੇ ਖੁੱਲ੍ਹ ਕੇ ਮਾਪਿਆਂ ਨਾਲ ਆਪਣੀਆਂ ਆਨਲਾਈਨ ਐਕਟਿਵਿਟੀ ਬਾਰੇ ਗੱਲ ਕਰ ਸਕਦੇ ਹਨ ਅਤੇ ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ ਲਿੰਕ ਜਾਂ ਮੈਸੇਜ ਦੇ ਸੰਪਰਕ ਵਿੱਚ ਆਉਣ ਤੇ ਸਹਾਇਤਾ ਲੈ ਸਕਦੇ ਹਨ।

ਸਾਂਝੀ ਜ਼ਿੰਮੇਵਾਰੀ ਦਾ ਇੱਕ ਮਹੱਤਵਪੂਰਨ ਹਿੱਸਾ **ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ** ਹੈ। ਮਾਪੇ ਬੱਚਿਆਂ ਨਾਲ ਨਿਰੰਤਰ ਸੰਚਾਰ ਕਰਕੇ ਉਨ੍ਹਾਂ ਦੀਆਂ ਆਦਤਾਂ, ਸਮੱਸਿਆਵਾਂ ਅਤੇ ਸਵਾਲਾਂ ਨੂੰ ਸਮਝ ਸਕਦੇ ਹਨ, ਜਦੋਂ ਕਿ ਬੱਚੇ ਭਰੋਸੇ ਨਾਲ ਮਾਪਿਆਂ ਨੂੰ ਸਾਰੀਆਂ ਜਾਣਕਾਰੀਆਂ ਸਾਂਝਾ ਕਰ ਸਕਦੇ ਹਨ।

ਸੰਖੇਪ ਵਿੱਚ, ਮਾਪਿਆਂ ਅਤੇ ਬੱਚਿਆਂ ਵਿਚਕਾਰ ਸਾਂਝੀ ਜ਼ਿੰਮੇਵਾਰੀ ਸਿਰਫ਼ ਸੁਰੱਖਿਆ ਲਈ ਨਹੀਂ, ਬਲਕਿ ਬੱਚਿਆਂ ਦੇ ਨੈਤਿਕ ਵਿਕਾਸ, ਜ਼ਿੰਮੇਵਾਰ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂ ਅਤੇ ਆਤਮ-ਨਿਰਭਰਤਾ ਲਈ ਵੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਸ ਤਰੀਕੇ ਨਾਲ ਬੱਚੇ ਸੁਰੱਖਿਅਤ, ਸਮਰਥ ਅਤੇ ਸੂਝਵਾਨ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂਕਾਰ ਬਣਦੇ ਹਨ।

15. ਐਮਰਜੈਂਸੀ ਸਥਿਤੀਆਂ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਆ ਬਰਕਰਾਰ ਰੱਖਣ ਦੌਰਾਨ ਬੱਚੇ ਅਤੇ ਮਾਪੇ ਕਈ ਵਾਰੀ **ਐਮਰਜੈਂਸੀ ਸਥਿਤੀਆਂ** ਦਾ ਸਾਹਮਣਾ ਕਰ ਸਕਦੇ ਹਨ। ਇਹ ਸਥਿਤੀਆਂ ਸਿਰਫ਼ ਭੌਤਿਕ ਹਾਦਸਿਆਂ ਤੱਕ ਸੀਮਿਤ ਨਹੀਂ ਹੁੰਦੀਆਂ, ਬਲਕਿ ਸਾਈਬਰ ਖ਼ਤਰੇ, ਫਰਾਡ, ਹੈਕਿੰਗ, ਅਣਜਾਣ ਲਿੰਕ ਅਤੇ ਨਕਲੀ ਜਾਣਕਾਰੀ ਨਾਲ ਵੀ ਜੁੜੀਆਂ ਹੋ ਸਕਦੀਆਂ ਹਨ। ਐਮਰਜੈਂਸੀ ਸਥਿਤੀਆਂ ਵਿੱਚ ਸਹੀ ਤਰੀਕੇ ਨਾਲ ਕਾਰਵਾਈ ਕਰਨ ਲਈ ਪਹਿਲਾਂ ਉਨ੍ਹਾਂ ਨੂੰ ਸਮਝਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਸਭ ਤੋਂ ਪਹਿਲਾਂ, **ਸਾਈਬਰ ਧੋਖਾਧੜੀ ਅਤੇ ਫਰਾਡ** ਐਮਰਜੈਂਸੀ ਸਥਿਤੀਆਂ ਹਨ। ਬੱਚੇ ਕਿਸੇ ਨਕਲੀ ਈਮੇਲ, ਫਿਸ਼ਿੰਗ ਲਿੰਕ ਜਾਂ OTP ਮੰਗਣ ਵਾਲੇ ਮੈਸੇਜ ‘ਤੇ ਕਲਿੱਕ ਕਰ ਦੇਣ। ਇਸ ਤਰ੍ਹਾਂ ਦੇ ਮਾਮਲਿਆਂ ਵਿੱਚ ਤੁਰੰਤ ਕਾਰਵਾਈ ਜ਼ਰੂਰੀ ਹੈ। ਬੱਚੇ ਨੂੰ ਸਿੱਖਾਇਆ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਅਣਜਾਣ ਲਿੰਕ ‘ਤੇ ਕਲਿੱਕ ਨਾ ਕਰਨ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰਨ ਅਤੇ ਮਾਪਿਆਂ ਜਾਂ ਅਧਿਆਪਕਾਂ ਨੂੰ ਤੁਰੰਤ ਜਾਣੂ ਕਰਨ।

ਇਸ ਤੋਂ ਇਲਾਵਾ, **ਹੈਕਿੰਗ ਅਤੇ ਅਕਾਊਂਟ ਕੰਪ੍ਰੋਮਾਈਜ਼** ਵੀ ਐਮਰਜੈਂਸੀ ਸਥਿਤੀ ਹੈ। ਜੇ ਬੱਚੇ ਦੇ ਆਨਲਾਈਨ ਖਾਤੇ ਹੈਕ ਹੋ ਜਾਂਦੇ ਹਨ, ਤਾਂ ਤੁਰੰਤ ਪਾਸਵਰਡ ਬਦਲੋ, 2FA ਲਾਗੂ ਕਰੋ ਅਤੇ ਬਰੋਸੇਮੰਦ ਸਰਵਿਸ ਪ੍ਰਦਾਤਾ ਨਾਲ ਸੰਪਰਕ ਕਰੋ। ਇਸ ਨਾਲ ਖਾਤੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਚੋਰੀ ਰੋਕੀ ਜਾ ਸਕਦੀ ਹੈ।

ਅਣਜਾਣ ਵਿਅਕਤੀਆਂ ਨਾਲ ਸੰਪਰਕ ਵੀ ਖ਼ਤਰਨਾਕ ਸਥਿਤੀ ਬਣ ਸਕਦੀ ਹੈ। ਬੱਚੇ ਕਈ ਵਾਰੀ ਚੈਟ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਜਾਂ ਗੇਮਿੰਗ ਪਲੇਟਫਾਰਮਾਂ ‘ਤੇ ਅਣਜਾਣ ਲੋਕਾਂ ਨਾਲ ਗੱਲਬਾਤ ਕਰ ਲੈਂਦੇ ਹਨ। ਮਾਪਿਆਂ ਨੂੰ ਬੱਚਿਆਂ ਨੂੰ ਸਮਝਾਉਣਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਕਿਸੇ ਵੀ ਵਿਅਕਤੀ ਨਾਲ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰਨ ਅਤੇ ਅਣਜਾਣ ਸੰਪਰਕ ਮਿਲਣ ਤੇ ਤੁਰੰਤ ਸਹਾਇਤਾ ਮੰਗਣ।

ਮਾਲਵੇਅਰ ਅਤੇ ਵਾਇਰਸ ਅਟੈਕਸ ਵੀ ਐਮਰਜੈਂਸੀ ਦੀ ਸ਼੍ਰੇਣੀ ਵਿੱਚ ਆਉਂਦੇ ਹਨ। ਬੱਚੇ ਅਣਜਾਣ ਫਾਈਲਾਂ ਡਾਊਨਲੋਡ ਕਰ ਲੈਂਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਡਿਵਾਈਸ ਸੰਕ੍ਰਮਿਤ ਹੋ ਸਕਦਾ ਹੈ। ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਐਂਟੀਵਾਇਰਸ ਸਾਫਟਵੇਅਰ ਦੀ ਵਰਤੋਂ ਅਤੇ ਮਾਪਿਆਂ/ਅਧਿਆਪਕਾਂ ਦੀ ਸਹਾਇਤਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ।

ਇਸਦੇ ਨਾਲ, **ਐਮਰਜੈਂਸੀ ਨੰਬਰ ਅਤੇ ਰਿਪੋਰਟਿੰਗ ਚੈਨਲਾਂ** ਦੀ ਜਾਣਕਾਰੀ ਵੀ ਬਹੁਤ ਅਹੰਸਭਾਗ ਹੈ। ਜਿਵੇਂ ਕਿ Cyber Crime Portal, 1930 Helpline, ਬੈਂਕ ਜਾਂ ਐਪ ਸਹਾਇਤਾ ਨੰਬਰ। ਮਾਪੇ ਅਤੇ ਬੱਚੇ ਇਹ ਜਾਣੂ ਹੋਣ ਨਾਲ ਤੁਰੰਤ ਕਾਰਵਾਈ ਕਰ ਸਕਦੇ ਹਨ।

ਐਮਰਜੈਂਸੀ ਸਥਿਤੀਆਂ ਆਨਲਾਈਨ ਅਤੇ ਡਿਜ਼ਿਟਲ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਆ ਲਈ ਚੁਣੌਤੀਪੂਰਨ ਹਨ। ਮਾਪਿਆਂ ਅਤੇ ਬੱਚਿਆਂ ਨੂੰ ਸਾਵਧਾਨੀ, ਨਿਗਰਾਨੀ, ਤੁਰੰਤ ਕਾਰਵਾਈ, ਸਹੀ ਸਲਾਹ ਅਤੇ ਰਿਪੋਰਟਿੰਗ ਚੈਨਲਾਂ ਦੀ ਜਾਣਕਾਰੀ ਨਾਲ ਤਿਆਰ ਰਹਿਣਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਉਪਾਅਵਾਂ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਜ਼ਿੰਮੇਵਾਰ ਅਤੇ ਨਿਰਭਰਯੋਗ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂਕਾਰ ਬਣਾਉਂਦੇ ਹਨ।

ਤੁਰੰਤ ਕੀ ਕਰਨਾ ਹੈ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚੇ ਕਈ ਵਾਰੀ ਅਣਜਾਣ ਖ਼ਤਰੇ, ਫਰਾਡ, ਹੈਕਿੰਗ, ਫਿਸ਼ਿੰਗ ਜਾਂ ਅਣਜਾਣ ਲਿੰਕਾਂ ਦਾ ਸਾਹਮਣਾ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਬੱਚਿਆਂ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਲਈ ਸਭ ਤੋਂ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਉਹ ਜਾਣਣ ਕਿ **ਤੁਰੰਤ ਕੀ ਕਰਨਾ** ਚਾਹੀਦਾ ਹੈ। ਸਹੀ ਅਤੇ ਤੇਜ਼ ਕਾਰਵਾਈ ਨਾਲ ਖ਼ਤਰੇ ਨੂੰ ਘਟਾਇਆ ਜਾ ਸਕਦਾ ਹੈ ਅਤੇ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਡਿਵਾਈਸ ਅਤੇ ਆਨਲਾਈਨ ਖਾਤਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਬਣਾਈ ਰੱਖੀ ਜਾ ਸਕਦੀ ਹੈ।

1. ਜੇ ਬੱਚੇ ਕਿਸੇ ਅਣਜਾਣ ਲਿੰਕ, ਫਿਸ਼ਿੰਗ ਮੈਸੇਜ ਜਾਂ ਨਕਲੀ ਈਮੇਲ ਦਾ ਸਾਹਮਣਾ ਕਰਦੇ ਹਨ, ਤਾਂ **ਕਿਸੇ ਵੀ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ**। ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਪਾਸਵਰਡ ਜਾਂ OTP ਸਾਂਝਾ ਨਾ ਕਰੋ। ਇਸ ਤੁਰੰਤ ਬੱਚੇ ਨੂੰ ਆਪਣੇ ਮਾਪਿਆਂ ਜਾਂ ਅਧਿਆਪਕਾਂ ਨੂੰ ਸੂਚਿਤ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਖੁੱਲ੍ਹਾ ਸੰਚਾਰ ਇਸ ਸਮੇਂ ਬੱਚੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਵਿੱਚ ਸਹਾਇਕ ਹੁੰਦਾ ਹੈ।
2. ਜੇ ਖਾਤਾ ਹੈਕ ਹੋ ਜਾਂਦਾ ਹੈ ਜਾਂ ਪਾਸਵਰਡ ਚੋਰੀ ਹੋ ਜਾਂਦਾ ਹੈ, ਤਾਂ ਤੁਰੰਤ **ਪਾਸਵਰਡ ਬਦਲੋ ਅਤੇ 2FA ਲਾਗੂ ਕਰੋ**। ਇਹ ਕਿਸੇ ਵੀ ਅਣਧਿਕਾਰਤ ਦਾਖਲੇ ਤੋਂ ਖਾਤੇ ਨੂੰ ਬਚਾਉਂਦਾ ਹੈ। ਹੈਕਿੰਗ ਹੋਣ ਦੀ ਸਥਿਤੀ ਵਿੱਚ, ਬੱਚੇ ਅਤੇ ਮਾਪੇ ਲਾਗੂ ਸਰਵਿਸ ਪ੍ਰਦਾਤਾ ਜਾਂ ਸਪੋਰਟ ਟੀਮ ਨਾਲ ਤੁਰੰਤ ਸੰਪਰਕ ਕਰਕੇ ਰਿਪੋਰਟ ਕਰ ਸਕਦੇ ਹਨ।
3. ਜੇ ਡਿਵਾਈਸ ਵਿੱਚ ਮਾਲਵੇਅਰ ਜਾਂ ਵਾਇਰਸ ਦਾ ਸੰਕ੍ਰਮਣ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਤੁਰੰਤ **ਐਂਟੀਵਾਇਰਸ ਸਕੈਨ ਕਰੋ ਅਤੇ ਸੰਕ੍ਰਮਿਤ ਫਾਈਲਾਂ ਨੂੰ ਰਿਮੂਵ ਕਰੋ**। ਡਿਵਾਈਸ ਨੂੰ ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਅਤੇ ਸੁਰੱਖਿਅਤ ਐਪਸ ਨਾਲ ਸੁਰੱਖਿਅਤ ਬਣਾਓ।
4. ਜੇ ਅਣਜਾਣ ਵਿਅਕਤੀ ਚੈਟ ਜਾਂ ਮੈਸੇਜ ਕਰ ਰਿਹਾ ਹੈ, ਤਾਂ ਤੁਰੰਤ **ਸੰਪਰਕ ਬੰਦ ਕਰੋ ਅਤੇ ਮਾਪਿਆਂ/ਅਧਿਆਪਕਾਂ ਨੂੰ ਜਾਣੂ ਕਰੋ**। ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਵਿਅਕਤੀ ਨਾਲ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰੋ।

5. ਸਾਈਬਰ ਅਪਰਾਧ ਜਾਂ ਸੰਕਟ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਬੱਚੇ, ਮਾਪੇ ਅਤੇ ਅਧਿਆਪਕ **ਸਰਕਾਰੀ ਰਿਪੋਰਟਿੰਗ ਚੈਨਲਾਂ** ਵਰਗੇ Cyber Crime Portal ਜਾਂ 1930 Helpline ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਤੁਰੰਤ ਰਿਪੋਰਟਿੰਗ ਨਾਲ ਕਾਰਵਾਈ ਤੇਜ਼ ਹੋ ਜਾਂਦੀ ਹੈ ਅਤੇ ਖ਼ਤਰਾ ਘਟਦਾ ਹੈ।

ਸੰਖੇਪ ਵਿੱਚ, ਅਣਜਾਣ ਖ਼ਤਰਿਆਂ, ਹੈਕਿੰਗ, ਫਰਾਡ, ਮਾਲਵੇਅਰ ਜਾਂ ਅਣਜਾਣ ਸੰਪਰਕ ਦੇ ਮਾਮਲਿਆਂ ਵਿੱਚ **ਤੁਰੰਤ ਕਾਰਵਾਈ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਸ ਵਿੱਚ ਬੱਚਿਆਂ ਦੀ ਸੂਚਨਾ, ਪਾਸਵਰਡ ਬਦਲਣਾ, 2FA ਲਾਗੂ ਕਰਨਾ, ਡਿਵਾਈਸ ਸੁਰੱਖਿਆ, ਅਣਜਾਣ ਵਿਅਕਤੀ ਨਾਲ ਸੰਪਰਕ ਬੰਦ ਕਰਨਾ ਅਤੇ ਰਿਪੋਰਟਿੰਗ ਚੈਨਲਾਂ ਦਾ ਸਹੀ ਵਰਤੋਂ ਸ਼ਾਮਲ ਹੈ। ਇਹ ਉਪਾਅਵਾਂ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਨਿਰਭਰਯੋਗ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂਕਾਰ ਬਣਾਉਂਦੇ ਹਨ।

Screenshots, Evidence ਸੰਭਾਲਣਾ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚੇ ਕਈ ਵਾਰੀ ਫਰਾਡ, ਫਿਸ਼ਿੰਗ, ਹੈਕਿੰਗ, ਨਕਲੀ ਖ਼ਬਰਾਂ ਜਾਂ ਅਣਜਾਣ ਵਿਅਕਤੀਆਂ ਨਾਲ ਸੰਪਰਕ ਵਿੱਚ ਆ ਸਕਦੇ ਹਨ। ਐਸੀਆਂ ਸਥਿਤੀਆਂ ਵਿੱਚ **Screenshots ਅਤੇ Evidence ਸੰਭਾਲਣਾ** ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਇਹ ਨਾਂ ਸਿਰਫ਼ ਸੁਰੱਖਿਆ ਲਈ ਜ਼ਰੂਰੀ ਹੈ, ਬਲਕਿ ਕਾਰਵਾਈ ਕਰਨ ਅਤੇ ਖ਼ਤਰੇ ਨੂੰ ਰੋਕਣ ਲਈ ਵੀ ਸਹਾਇਕ ਹੈ। Screenshots ਅਤੇ ਹੋਰ ਡਿਜ਼ਿਟਲ ਸਬੂਤ ਤੁਹਾਡੇ ਬੱਚਿਆਂ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਲਈ ਸੁਰੱਖਿਆ ਦਾ ਇੱਕ ਮਜ਼ਬੂਤ ਸਾਧਨ ਬਣ ਜਾਂਦੇ ਹਨ।

1. ਜਦੋਂ ਵੀ ਬੱਚਾ ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ, ਸ਼ੱਕੀ ਲਿੰਕ ਜਾਂ ਨਕਲੀ ਮੈਸੇਜ ਦਾ ਸਾਹਮਣਾ ਕਰਦਾ ਹੈ, ਉਸ ਨੂੰ **ਤੁਰੰਤ Screenshot ਲੈਣੀ ਚਾਹੀਦੀ ਹੈ**। ਇਹ Screenshot ਮੈਸੇਜ, ਈਮੇਲ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਚੈਟ ਜਾਂ ਅਣਜਾਣ ਲਿੰਕ ਦੀ ਪੂਰੀ ਜਾਣਕਾਰੀ ਦਰਸਾਉਂਦੀ ਹੈ। Screenshot ਵਿੱਚ ਡਿਵਾਈਸ, ਡੇਟ ਅਤੇ ਸਮਾਂ ਵੀ ਦਰਸਾਇਆ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ, ਤਾਂ ਜੋ ਇਹ ਸਬੂਤ ਪ੍ਰਮਾਣਿਕ ਬਣੇ।
2. Screenshots ਨੂੰ **ਸੁਰੱਖਿਅਤ ਥਾਂ ਤੇ ਸੰਭਾਲਣਾ** ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਇਹ ਮਾਪਿਆਂ ਦੇ ਡਿਵਾਈਸ, ਕਲਾਉਡ ਸਟੋਰੇਜ ਜਾਂ ਪਾਸਵਰਡ-ਸੁਰੱਖਿਅਤ ਫੋਲਡਰ ਵਿੱਚ ਰੱਖੇ ਜਾ ਸਕਦੇ ਹਨ। ਇਸ ਨਾਲ ਇਹ ਡਿਜ਼ਿਟਲ ਸਬੂਤ ਬਿਨਾਂ ਕਿਸੇ ਖ਼ਤਰੇ ਦੇ ਸੁਰੱਖਿਅਤ ਰਹਿੰਦੇ ਹਨ ਅਤੇ ਜਦੋਂ ਲੋੜ ਪਏ, ਤੁਰੰਤ ਵਰਤੇ ਜਾ ਸਕਦੇ ਹਨ।

3. Screenshots ਅਤੇ ਹੋਰ Evidence ਨੂੰ ਵਿਸ਼ੇਸ਼ ਤਰੀਕੇ ਨਾਲ ਸੰਭਾਲਣਾ ਅਤੇ ਸਹੀ ਲੇਬਲਿੰਗ ਕਰਨਾ ਜ਼ਰੂਰੀ ਹੈ। ਹਰ Screenshot ਨੂੰ ਸਬੰਧਿਤ ਤਾਰੀਖ, ਸਮਾਂ ਅਤੇ ਸਥਿਤੀ ਦੇ ਨਾਲ ਸੇਵ ਕਰੋ। ਇਸ ਤਰੀਕੇ ਨਾਲ ਬਾਅਦ ਵਿੱਚ ਕੋਈ ਗਲਤਫ਼ਹਿਮੀ ਨਹੀਂ ਹੁੰਦੀ ਅਤੇ ਜੇ ਕਾਰਵਾਈ ਕਰਨੀ ਪਏ, ਤਾਂ ਸਬੂਤ ਸਪਸ਼ਟ ਹੋਵੇ।
4. ਜੇ ਬੱਚੇ ਨੂੰ Cyber Crime ਜਾਂ ਸਕੂਲ/ਸਮਾਜਿਕ ਸੰਬੰਧੀ ਸ਼ਿਕਾਇਤ ਕਰਨੀ ਪਵੇ, ਤਾਂ Screenshots ਅਤੇ Evidence ਰਿਪੋਰਟਿੰਗ ਵਿੱਚ ਵਰਤੋਂ ਕਰਨਾ ਬਹੁਤ ਮਦਦਗਾਰ ਹੁੰਦਾ ਹੈ। ਇਹ ਸਬੂਤ ਰਿਪੋਰਟ ਨੂੰ ਭਰੋਸੇਮੰਦ ਅਤੇ ਕਾਰਵਾਈਯੋਗ ਬਣਾਉਂਦਾ ਹੈ। ਜਿਵੇਂ ਕਿ Cyber Crime Portal ਜਾਂ ਸਕੂਲ ਦੀ ਸਹਾਇਤਾ ਟੀਮ ਨੂੰ Screenshots ਦੇ ਕੇ ਬੱਚਾ ਆਪਣੀ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਵਾ ਸਕਦਾ ਹੈ।

ਸੰਖੇਪ ਵਿੱਚ, Screenshots ਅਤੇ Evidence ਸੰਭਾਲਣਾ ਇੱਕ ਸੁਰੱਖਿਆ ਅਤੇ ਸਬੂਤ ਪ੍ਰਬੰਧਨ ਪ੍ਰਕਿਰਿਆ ਹੈ। ਇਹ ਬੱਚਿਆਂ ਨੂੰ ਆਨਲਾਈਨ ਖ਼ਤਰੇ ਤੋਂ ਸੁਰੱਖਿਅਤ ਰੱਖਣ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਕਾਰਵਾਈ ਕਰਨ ਅਤੇ ਬੱਚਿਆਂ ਨੂੰ ਨਿਰਭਰਯੋਗ ਬਣਾਉਣ ਵਿੱਚ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਸਹੀ ਤਰੀਕੇ ਨਾਲ Screenshots ਲੈਣਾ, ਸੁਰੱਖਿਅਤ ਥਾਂ ਤੇ ਸੰਭਾਲਣਾ, ਲੇਬਲਿੰਗ ਕਰਨਾ ਅਤੇ ਜ਼ਰੂਰੀ ਕਾਰਵਾਈ ਲਈ ਵਰਤਣਾ ਬੱਚਿਆਂ ਦੀ ਡਿਜ਼ਿਟਲ ਸੁਰੱਖਿਆ ਨੂੰ ਮਜ਼ਬੂਤ ਬਣਾਉਂਦਾ ਹੈ।

ਮਦਦ ਲਈ ਕਿਥੇ ਸੰਪਰਕ ਕਰਨਾ

ਆਨਲਾਈਨ ਦੁਨੀਆ ਵਿੱਚ ਬੱਚੇ ਕਈ ਵਾਰੀ ਫਿਸ਼ਿੰਗ, ਫਰਾਡ, ਹੈਕਿੰਗ, ਨਕਲੀ ਖਬਰਾਂ, ਅਣਜਾਣ ਵਿਅਕਤੀਆਂ ਨਾਲ ਸੰਪਰਕ ਜਾਂ ਅਸੁਰੱਖਿਅਤ ਐਪਸ ਵਰਤਣ ਦੇ ਖ਼ਤਰੇ ਦਾ ਸਾਹਮਣਾ ਕਰਦੇ ਹਨ। ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਸਥਿਤੀ ਵਿੱਚ **ਤੁਰੰਤ ਅਤੇ ਭਰੋਸੇਮੰਦ ਸਹਾਇਤਾ ਲੈਣਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ**। ਬੱਚਿਆਂ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਨੂੰ ਜਾਣਨਾ ਚਾਹੀਦਾ ਹੈ ਕਿ ਮਦਦ ਲਈ ਕਿੱਥੇ ਸੰਪਰਕ ਕੀਤਾ ਜਾ ਸਕਦਾ ਹੈ, ਤਾਂ ਜੋ ਖ਼ਤਰੇ ਨੂੰ ਘਟਾਇਆ ਜਾ ਸਕੇ ਅਤੇ ਡਿਜ਼ਿਟਲ ਸੁਰੱਖਿਆ ਯਕੀਨੀ ਬਣਾਈ ਜਾ ਸਕੇ।

1. **ਸਰਕਾਰੀ Cyber Crime Portal (<https://cybercrime.gov.in/>)** ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਸਹਾਇਤਾ ਕੇਂਦਰ ਹੈ। ਇੱਥੇ ਬੱਚੇ ਜਾਂ ਮਾਪੇ ਕਿਸੇ ਵੀ ਆਨਲਾਈਨ ਧੋਖਾਧੜੀ, ਹੈਕਿੰਗ, ਫਰਾਡ, ਫਿਸ਼ਿੰਗ ਜਾਂ ਨਕਲੀ ਖਬਰਾਂ ਦੀ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਵਾ ਸਕਦੇ ਹਨ। ਇਹ ਪੋਰਟਲ ਤੁਰੰਤ ਕਾਰਵਾਈ ਅਤੇ ਮਾਨੀਟਰਿੰਗ ਦੀ ਸੁਵਿਧਾ ਦਿੰਦਾ ਹੈ। Cyber Crime Portal 24×7 ਉਪਲਬਧ ਹੈ ਅਤੇ ਵਿਭਿੰਨ ਸ਼ਿਕਾਇਤਾਂ ਲਈ ਸਹੀ ਸਹਾਇਤਾ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ।

2. **1930 Helpline** ਵੀ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਇਹ ਹੇਲਪਲਾਈਨ ਬੱਚਿਆਂ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਲਈ ਸਲਾਹ, ਰਾਹਨੁਮਾਈ ਅਤੇ ਸੁਰੱਖਿਆ ਸਬੰਧੀ ਜਾਣਕਾਰੀ ਪ੍ਰਦਾਨ ਕਰਦੀ ਹੈ। ਜੇ ਬੱਚੇ ਕਿਸੇ ਅਣਜਾਣ ਵਿਅਕਤੀ ਨਾਲ ਚੈਟ ਕਰ ਰਿਹਾ ਹੈ, ਫਿਸ਼ਿੰਗ ਲਿੰਕ ਮਿਲਿਆ ਹੈ ਜਾਂ ਸਾਈਬਰ ਬੁੱਲੀਅੰਗ ਦਾ ਸਾਹਮਣਾ ਕਰ ਰਿਹਾ ਹੈ, ਤਾਂ 1930 Helpline ਤੁਰੰਤ ਸਹਾਇਤਾ ਦੇ ਸਕਦੀ ਹੈ।
3. ਬੱਚੇ ਆਪਣੇ ਸਕੂਲ ਦੇ **ਅਧਿਆਪਕ ਜਾਂ IT ਸਮਰਥਕ ਟੀਮ** ਨਾਲ ਵੀ ਸੰਪਰਕ ਕਰ ਸਕਦੇ ਹਨ। ਸਕੂਲ ਅਕਸਰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਨਿਯਮ, ਪੋਰੈਂਟਲ ਕੰਟਰੋਲ ਅਤੇ ਮੀਟਿੰਗ ਸੁਰੱਖਿਆ ਲਈ ਮਦਦਗਾਰ ਹੁੰਦਾ ਹੈ। ਬੱਚੇ ਸਕੂਲ ਨਾਲ ਸੰਪਰਕ ਕਰਕੇ ਆਪਣੀ ਸੁਰੱਖਿਆ ਯਕੀਨੀ ਬਣਾਉਂਦੇ ਹਨ ਅਤੇ ਸਮੱਸਿਆ ਦਾ ਤੇਜ਼ ਹੱਲ ਲੱਭ ਸਕਦੇ ਹਨ।
4. ਜੇ ਕਿਸੇ ਫਰਾਡ, OTP ਚੋਰੀ ਜਾਂ ਬੈਂਕ ਸੰਬੰਧੀ ਖ਼ਤਰੇ ਦਾ ਸਾਹਮਣਾ ਹੋਵੇ, ਤਾਂ **ਬੈਂਕ ਜਾਂ ਐਪ ਸਹਾਇਤਾ ਨੰਬਰ** ਨੂੰ ਤੁਰੰਤ ਕਾਲ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਇਹ ਮਾਲੀ ਖ਼ਤਰੇ ਤੋਂ ਸੁਰੱਖਿਆ ਦੇਣ ਵਿੱਚ ਬਹੁਤ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਹੈ।

ਸੰਖੇਪ ਵਿੱਚ, ਬੱਚਿਆਂ, ਮਾਪਿਆਂ ਅਤੇ ਅਧਿਆਪਕਾਂ ਲਈ ਮਦਦ ਲਈ ਸੰਪਰਕ ਕਰਨਾ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। Cyber Crime Portal, 1930 Helpline, ਸਕੂਲ ਦੇ ਅਧਿਆਪਕ/IT ਟੀਮ ਅਤੇ ਬੈਂਕ ਸਹਾਇਤਾ ਨੰਬਰ ਵਰਗੇ ਭਰੋਸੇਮੰਦ ਸਰੋਤ ਤੁਰੰਤ ਕਾਰਵਾਈ ਅਤੇ ਸੁਰੱਖਿਆ ਯਕੀਨੀ ਬਣਾਉਂਦੇ ਹਨ। ਇਹ ਉਪਾਅਵਾਂ ਬੱਚਿਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ, ਜ਼ਿੰਮੇਵਾਰ ਅਤੇ ਨਿਰਭਰਯੋਗ ਡਿਜ਼ਿਟਲ ਵਰਤੋਂਕਾਰ ਬਣਾਉਂਦੇ ਹਨ।

16. ਭਾਰਤ ਸਰਕਾਰ ਦੇ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਸ਼ਿਕਾਇਤ ਪੋਰਟਲ ਤੇ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਵਾਉਣ ਦਾ ਤਰੀਕਾ

Cybercrime.gov.in 'ਤੇ ਸ਼ਿਕਾਇਤ ਕਿਵੇਂ ਦਰਜ ਕਰੀਏ

ਕਦਮ 1: ਵੈੱਬਸਾਈਟ ਖੋਲ੍ਹੋ

- 👉 ਆਪਣੇ ਮੋਬਾਈਲ ਜਾਂ ਕੰਪਿਊਟਰ 'ਤੇ ਬ੍ਰਾਊਜ਼ਰ ਖੋਲ੍ਹੋ
- 👉 www.cybercrime.gov.in ਲਿਖੋ ਅਤੇ Enter ਦਬਾਓ

ਕਦਮ 2: "File a Complaint" 'ਤੇ ਕਲਿੱਕ ਕਰੋ

- ਹੋਮ ਪੇਜ 'ਤੇ "File a Complaint" ਦਾ ਵਿਕਲਪ ਮਿਲੇਗਾ
- ਉਸ 'ਤੇ ਕਲਿੱਕ ਕਰੋ

ਕਦਮ 3: ਸ਼ਿਕਾਇਤ ਦੀ ਕਿਸਮ ਚੁਣੋ

ਤੁਹਾਨੂੰ ਦੋ ਵਿਕਲਪ ਮਿਲਣਗੇ:

1. Report Women/Child Related Crime

👉 ਜੇ ਅਪਰਾਧ ਔਰਤ ਜਾਂ ਬੱਚੇ ਨਾਲ ਸੰਬੰਧਿਤ ਹੈ (ਜਿਵੇਂ: ਧਮਕੀਆਂ, ਅਸ਼ਲੀਲ ਤਸਵੀਰਾਂ ਆਦਿ)

2. Report Other Cyber Crime

👉 ਜੇ ਅਪਰਾਧ ਹੋਰ ਕਿਸੇ ਕਿਸਮ ਦਾ ਹੈ (ਜਿਵੇਂ:

- Online Fraud
- UPI / ATM Fraud
- Facebook / Instagram Hack
- Fake Calls / Messages)

ਉਚਿਤ ਵਿਕਲਪ 'ਤੇ ਕਲਿੱਕ ਕਰੋ

ਕਦਮ 4: Login ਜਾਂ Register ਕਰੋ

- ਮੋਬਾਈਲ ਨੰਬਰ ਦਰਜ ਕਰੋ
- OTP ਆਵੇਗਾ → OTP ਭਰੋ
- Login ਹੋ ਜਾਵੇਗਾ

ਕਦਮ 5: ਸ਼ਿਕਾਇਤ ਦੀ ਪੂਰੀ ਜਾਣਕਾਰੀ ਭਰੋ

ਹੁਣ ਫਾਰਮ ਵਿੱਚ ਇਹ ਜਾਣਕਾਰੀ ਭਰੋ:

- ਘਟਨਾ ਦੀ ਤਾਰੀਖ ਅਤੇ ਸਮਾਂ
- ਅਪਰਾਧ ਦੀ ਪੂਰੀ ਜਾਣਕਾਰੀ
- ਜਿਸ ਅਕਾਊਂਟ / ਨੰਬਰ ਤੋਂ ਧੋਖਾਧੜੀ ਹੋਈ
- ਨੁਕਸਾਨ ਹੋਈ ਰਕਮ (ਜੇ ਹੋਈ ਹੈ)

ਜੇ ਤੁਹਾਡੇ ਕੋਲ Screenshot, Photo, Video, Chat, Bank Statement ਆਦਿ ਹਨ ਤਾਂ ਉਹ ਵੀ Upload ਕਰੋ

ਕਦਮ 6: Submit ਕਰੋ

- ਸਾਰੀ ਜਾਣਕਾਰੀ ਚੈੱਕ ਕਰੋ
- Submit ਬਟਨ ਦਬਾਓ

✓ Submit ਕਰਨ ਤੋਂ ਬਾਅਦ ਤੁਹਾਨੂੰ Complaint ID ਮਿਲੇਗੀ

👉 ਇਸ ID ਨਾਲ ਤੁਸੀਂ ਆਪਣੀ ਸ਼ਿਕਾਇਤ ਦੀ ਸਥਿਤੀ Track ਕਰ ਸਕਦੇ ਹੋ

ਜ਼ਰੂਰੀ ਜਾਣਕਾਰੀ

- Cyber Crime Helpline Number: 1930
(Financial Fraud ਲਈ ਤੁਰੰਤ ਕਾਲ ਕਰੋ)

17. ਆਨਲਾਈਨ ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ ਬਾਰੇ ਜਾਣਕਾਰੀ

ਆਨਲਾਈਨ ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ

ਅੱਜ ਦੇ ਡਿਜੀਟਲ ਯੁੱਗ ਵਿੱਚ ਬੱਚੇ ਮੋਬਾਈਲ ਫੋਨ, ਟੈਬਲੈਟ ਅਤੇ ਇੰਟਰਨੈੱਟ ਦਾ ਵੱਡੇ ਪੱਧਰ 'ਤੇ ਇਸਤੇਮਾਲ ਕਰ ਰਹੇ ਹਨ। ਆਨਲਾਈਨ ਸਿੱਖਿਆ ਦੇ ਨਾਲ-ਨਾਲ ਸੋਸ਼ਲ ਮੀਡੀਆ, ਗੇਮਿੰਗ ਅਤੇ ਵੀਡੀਓ ਪਲੇਟਫਾਰਮ ਵੀ ਬੱਚਿਆਂ ਦੀ ਜ਼ਿੰਦਗੀ ਦਾ ਹਿੱਸਾ ਬਣ ਚੁੱਕੇ ਹਨ। ਪਰ ਇਸ ਨਾਲ ਕੁਝ ਖਤਰੇ ਵੀ ਜੁੜੇ ਹੋਏ ਹਨ, ਜਿਵੇਂ ਕਿ ਅਣਉਚਿਤ ਸਮੱਗਰੀ, ਆਨਲਾਈਨ ਧੋਖਾਧੜੀ, ਸਾਇਬਰ ਬੁਲਿੰਗ ਅਤੇ ਮੋਬਾਈਲ ਦੀ ਅਤਿ ਵਰਤੋਂ।

ਇਨ੍ਹਾਂ ਸਮੱਸਿਆਵਾਂ ਤੋਂ ਬੱਚਿਆਂ ਨੂੰ ਬਚਾਉਣ ਲਈ **ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ** ਬਹੁਤ ਮਦਦਗਾਰ ਸਾਬਤ ਹੁੰਦੀਆਂ ਹਨ। ਇਹ ਐਪਸ ਮਾਪਿਆਂ ਨੂੰ ਬੱਚਿਆਂ ਦੀ ਆਨਲਾਈਨ ਸਰਗਰਮੀਆਂ 'ਤੇ ਨਿਗਰਾਨੀ ਰੱਖਣ, ਸਮਾਂ ਸੀਮਿਤ ਕਰਨ ਅਤੇ ਅਣਚਾਹੀ ਸਮੱਗਰੀ ਨੂੰ ਰੋਕਣ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਦੀਆਂ ਹਨ।



ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ ਦੇ ਮੁੱਖ ਫਾਇਦੇ

- ਮੋਬਾਈਲ ਅਤੇ ਐਪ ਵਰਤੋਂ 'ਤੇ ਨਿਯੰਤਰਣ
- ਸਕ੍ਰੀਨ ਟਾਈਮ ਸੀਮਾ ਤੈਅ ਕਰਨਾ
- ਅਣਉਚਿਤ ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ ਵੀਡੀਓਜ਼ ਨੂੰ ਬਲੋਕ ਕਰਨਾ
- ਬੱਚੇ ਦੀ ਲੋਕੇਸ਼ਨ ਟ੍ਰੈਕ ਕਰਨਾ

- ਕਾਲ ਅਤੇ ਮੈਸੇਜ ਨਿਗਰਾਨੀ (ਕੁਝ ਐਪਸ ਵਿੱਚ)

ਵੱਖ-ਵੱਖ ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ ਬਾਰੇ ਜਾਣਕਾਰੀ

1. Google Family Link

- ◆ Android ਅਤੇ Chromebook ਲਈ ਉਪਯੋਗੀ
 - ◆ ਬੱਚੇ ਦੀ ਸਕ੍ਰੀਨ ਟਾਈਮ ਕੰਟਰੋਲ
 - ◆ ਐਪ ਇੰਸਟਾਲ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਮਾਪਿਆਂ ਦੀ ਮਨਜ਼ੂਰੀ
 - ◆ ਮੁਫਤ ਐਪ
- 👉 ਸਕੂਲ ਜਾਣ ਵਾਲੇ ਬੱਚਿਆਂ ਲਈ ਬਹੁਤ ਵਧੀਆ

2. Microsoft Family Safety

- ◆ Windows, Android ਅਤੇ Xbox ਲਈ
 - ◆ ਸਕ੍ਰੀਨ ਟਾਈਮ ਅਤੇ ਐਪ ਫਿਲਟਰ
 - ◆ ਲੋਕੇਸ਼ਨ ਸ਼ੇਅਰਿੰਗ
 - ◆ Email ਅਤੇ Calendar ਸੁਰੱਖਿਆ
- 👉 Microsoft ਡਿਵਾਈਸ ਵਰਤਣ ਵਾਲੇ ਪਰਿਵਾਰਾਂ ਲਈ ਉਪਯੋਗੀ

3. Kaspersky Safe Kids

- ◆ ਇੰਟਰਨੈੱਟ ਅਤੇ ਐਪ ਕੰਟਰੋਲ
 - ◆ GPS ਲੋਕੇਸ਼ਨ ਟ੍ਰੈਕਿੰਗ
 - ◆ YouTube ਸਰਚ ਮੋਨੀਟਰ
 - ◆ Android ਅਤੇ iOS ਲਈ ਉਪਲਬਧ
- 👉 ਸੁਰੱਖਿਆ 'ਤੇ ਧਿਆਨ ਦੇਣ ਵਾਲੇ ਮਾਪਿਆਂ ਲਈ ਵਧੀਆ

4. Norton Family

- ◆ ਵੈੱਬਸਾਈਟ ਅਤੇ ਸਰਚ ਇੰਜਨ ਫਿਲਟਰ
- ◆ ਸਕ੍ਰੀਨ ਟਾਈਮ ਮੈਨੇਜਮੈਂਟ
- ◆ Online Activity Report
- ◆ ਸਕੂਲੀ ਉਮਰ ਦੇ ਬੱਚਿਆਂ ਲਈ ਢੁੱਕਵਾਂ

5. Kidslox

- ◆ ਇੱਕ ਕਲਿੱਕ 'ਚ ਫੋਨ ਲੋਕ
- ◆ ਐਪ ਅਤੇ ਗੇਮ ਕੰਟਰੋਲ
- ◆ ਸਕ੍ਰੀਨ ਟਾਈਮ ਸੀਮਾ
- ◆ Android ਅਤੇ iOS ਦੇਵਾਂ ਲਈ

👉 ਛੋਟੇ ਬੱਚਿਆਂ ਲਈ ਸੌਖੀ ਐਪ

⚠ ਮਾਪਿਆਂ ਲਈ ਜ਼ਰੂਰੀ ਸਲਾਹ

- ਬੱਚਿਆਂ ਨਾਲ ਖੁੱਲ੍ਹ ਕੇ ਗੱਲਬਾਤ ਕਰੋ
- ਐਪ ਦੇ ਨਾਲ-ਨਾਲ ਭਰੋਸਾ ਵੀ ਬਣਾਓ
- ਉਮਰ ਦੇ ਅਨੁਸਾਰ ਕੰਟਰੋਲ ਲਗਾਓ
- ਬੱਚਿਆਂ ਨੂੰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਬਾਰੇ ਸਿੱਖਾਓ

ਪੈਰੈਂਟਲ ਕੰਟਰੋਲ ਐਪਸ ਮਾਪਿਆਂ ਲਈ ਇੱਕ ਮਜ਼ਬੂਤ ਸਾਧਨ ਹਨ, ਪਰ ਇਹ ਬੱਚਿਆਂ ਨਾਲ ਸਹੀ ਸੰਵਾਦ ਦੀ ਜਗ੍ਹਾ ਨਹੀਂ ਲੈ ਸਕਦੀਆਂ। ਸਹੀ ਐਪ ਦੀ ਚੋਣ ਅਤੇ ਸਮਝਦਾਰੀ ਨਾਲ ਵਰਤੋਂ ਕਰਕੇ ਅਸੀਂ ਆਪਣੇ ਬੱਚਿਆਂ ਨੂੰ ਡਿਜੀਟਲ ਦੁਨੀਆ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹਾਂ।

18. ਭਾਰਤ ਸਰਕਾਰ ਦੀ ਸੰਚਾਰ ਸਾਥੀ ਐਪ ਸੰਬੰਧੀ ਸੰਪੂਰਨ ਜਾਣਕਾਰੀ

ਸੰਚਾਰ ਸਾਥੀ ਐਪ (Sanchar Saathi) - ਸੰਪੂਰਨ ਜਾਣਕਾਰੀ

ਸੰਚਾਰ ਸਾਥੀ ਭਾਰਤ ਸਰਕਾਰ ਦੇ ਦੂਰਸੰਚਾਰ ਵਿਭਾਗ (Department of Telecommunications – DoT) ਵੱਲੋਂ ਸ਼ੁਰੂ ਕੀਤਾ ਗਿਆ ਇੱਕ ਮਹੱਤਵਪੂਰਨ ਡਿਜੀਟਲ ਉਪਰਾਲਾ ਹੈ। ਇਸ ਦਾ ਮੁੱਖ ਉਦੇਸ਼ ਨਾਗਰਿਕਾਂ ਨੂੰ ਮੋਬਾਈਲ ਸਿਮ ਕਾਰਡ, ਮੋਬਾਈਲ ਫੋਨ ਅਤੇ ਟੈਲੀਕਾਮ ਧੋਖਾਧੜੀ ਤੋਂ ਬਚਾਉਣਾ ਹੈ।

ਇਹ ਸੇਵਾ Sanchar Saathi Portal ਅਤੇ ਮੋਬਾਈਲ ਐਪ ਦੇ ਰੂਪ ਵਿੱਚ ਉਪਲਬਧ ਹੈ।



ਸੰਚਾਰ ਸਾਥੀ ਦਾ ਮੁੱਖ ਉਦੇਸ਼

- ਨਾਗਰਿਕਾਂ ਦੇ ਨਾਮ 'ਤੇ ਜਾਰੀ ਸਿਮ ਕਾਰਡਾਂ ਦੀ ਜਾਣਕਾਰੀ ਦੇਣਾ
- ਗੁੰਮ ਜਾਂ ਚੋਰੀ ਹੋਏ ਮੋਬਾਈਲ ਫੋਨ ਨੂੰ ਬਲੈਕ ਕਰਨਾ
- ਫਰਾਡ / ਨਕਲੀ ਕਾਲਾਂ ਅਤੇ ਮੈਸੇਜਾਂ ਤੋਂ ਬਚਾਅ
- ਟੈਲੀਕਾਮ ਸੇਵਾਵਾਂ ਵਿੱਚ ਪਾਰਦਰਸ਼ਤਾ ਲਿਆਉਣਾ

ਸੰਚਾਰ ਸਾਥੀ ਐਪ/ਪੋਰਟਲ ਦੀਆਂ ਮੁੱਖ ਸੇਵਾਵਾਂ

1. TAF COP (Know Your Mobile Connections)

ਇਸ ਸੇਵਾ ਰਾਹੀਂ:

- ਤੁਸੀਂ ਆਪਣੇ ਆਧਾਰ ਨੰਬਰ ਨਾਲ ਜੁੜੇ ਸਾਰੇ ਮੋਬਾਈਲ ਨੰਬਰਾਂ ਦੀ ਜਾਣਕਾਰੀ ਲੈ ਸਕਦੇ ਹੋ
- ਜੇ ਕੋਈ ਨੰਬਰ ਤੁਹਾਡੇ ਬਿਨਾਂ ਜਾਣਕਾਰੀ ਦੇ ਚਲ ਰਿਹਾ ਹੈ, ਤਾਂ ਤੁਸੀਂ ਉਸਦੀ ਸ਼ਿਕਾਇਤ ਕਰ ਸਕਦੇ ਹੋ

👉 ਇਹ ਸੇਵਾ ਨਕਲੀ ਜਾਂ ਗਲਤ ਸਿਮ ਕਾਰਡਾਂ ਨੂੰ ਰੋਕਣ ਵਿੱਚ ਮਦਦਗਾਰ ਹੈ

2. CEIR - ਗੁੰਮ/ਚੋਰੀ ਹੋਇਆ ਮੋਬਾਈਲ ਬਲੋਕ ਕਰਨਾ

ਜੇ ਤੁਹਾਡਾ ਮੋਬਾਈਲ ਫੋਨ:

- ਗੁੰਮ ਹੋ ਗਿਆ ਹੈ
- ਜਾਂ ਚੋਰੀ ਹੋ ਗਿਆ ਹੈ

ਤਾਂ ਤੁਸੀਂ:

- ਉਸਦਾ IMEI ਨੰਬਰ ਦਰਜ ਕਰਕੇ
- ਫੋਨ ਨੂੰ ਪੂਰੇ ਦੇਸ਼ ਵਿੱਚ ਬਲੋਕ ਕਰ ਸਕਦੇ ਹੋ

✓ ਬਲੋਕ ਹੋਣ ਤੋਂ ਬਾਅਦ ਉਹ ਫੋਨ ਕਿਸੇ ਵੀ ਨੈੱਟਵਰਕ 'ਤੇ ਵਰਤਿਆ ਨਹੀਂ ਜਾ ਸਕਦਾ

3. Chakshu - ਫਰਾਡ ਕਾਲਾਂ ਅਤੇ ਮੈਸੇਜ ਦੀ ਸ਼ਿਕਾਇਤ

ਇਸ ਫੀਚਰ ਨਾਲ ਤੁਸੀਂ:

- ਫਰਾਡ ਕਾਲ
- ਨਕਲੀ SMS
- ਝੂਠੇ KYC ਅਪਡੇਟ ਮੈਸੇਜ
- ਬੈਂਕ / UPI ਧੋਖਾਧੜੀ ਵਾਲੀਆਂ ਕਾਲਾਂ

ਦੀ ਰਿਪੋਰਟ ਕਰ ਸਕਦੇ ਹੋ

👉 ਇਸ ਨਾਲ ਸਰਕਾਰ ਨੂੰ ਫਰਾਡ ਨੰਬਰਾਂ 'ਤੇ ਕਾਰਵਾਈ ਕਰਨ ਵਿੱਚ ਮਦਦ ਮਿਲਦੀ ਹੈ

4. ਨਾਗਰਿਕਾਂ ਲਈ ਸੁਰੱਖਿਆ ਅਤੇ ਜਾਗਰੂਕਤਾ

- ਡਿਜੀਟਲ ਧੋਖਾਧੜੀ ਤੋਂ ਬਚਣ ਲਈ ਜਾਣਕਾਰੀ
- ਟੈਲੀਕਾਮ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਸਲਾਹਾਂ
- ਸਰਕਾਰ ਵੱਲੋਂ ਜਾਰੀ ਨਵੇਂ ਨਿਰਦੇਸ਼

ਸੰਚਾਰ ਸਾਥੀ ਐਪ ਕਿਵੇਂ ਵਰਤੀਏ?

1. ਮੋਬਾਈਲ 'ਚ **Sanchar Saathi App** ਇੰਸਟਾਲ ਕਰੋ ਜਾਂ ਪੋਰਟਲ ਖੋਲ੍ਹੋ
2. ਮੋਬਾਈਲ ਨੰਬਰ ਨਾਲ **OTP ਦੁਆਰਾ ਲੌਗਇਨ** ਕਰੋ
3. ਲੋੜ ਅਨੁਸਾਰ ਸੇਵਾ ਚੁਣੋ (TAFcop / CEIR / Chakshu)
4. ਜਾਣਕਾਰੀ ਭਰੋ ਅਤੇ Submit ਕਰੋ

ਸੰਚਾਰ ਸਾਥੀ ਦੇ ਫਾਇਦੇ

- ਨਾਗਰਿਕਾਂ ਲਈ ਮੁਫਤ ਸੇਵਾ
- ਮੋਬਾਈਲ ਅਤੇ ਸਿਮ ਸੁਰੱਖਿਆ
- ਫਰਾਡ 'ਤੇ ਤੇਜ਼ ਕਾਰਵਾਈ
- ਡਿਜੀਟਲ ਭਰੋਸਾ ਵਧਾਉਂਦੀ ਹੈ

ਮਹੱਤਵਪੂਰਨ ਸਲਾਹ

- ਆਪਣਾ ਆਧਾਰ ਅਤੇ OTP ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ
- ਸ਼ੱਕੀ ਕਾਲ ਜਾਂ ਮੈਸੇਜ ਦੀ ਤੁਰੰਤ ਰਿਪੋਰਟ ਕਰੋ
- ਸਿਰਫ਼ ਸਰਕਾਰੀ ਪੋਰਟਲ ਜਾਂ ਐਪ ਦੀ ਵਰਤੋਂ ਕਰੋ
-

ਸੰਚਾਰ ਸਾਥੀ ਐਪ ਭਾਰਤ ਸਰਕਾਰ ਵੱਲੋਂ ਨਾਗਰਿਕਾਂ ਦੀ ਟੈਲੀਕਾਮ ਸੁਰੱਖਿਆ ਲਈ ਇੱਕ ਬਹੁਤ ਹੀ ਲਾਭਦਾਇਕ ਅਤੇ ਭਰੋਸੇਯੋਗ ਪਹਲ ਹੈ। ਇਹ ਐਪ ਮੋਬਾਈਲ ਧੋਖਾਧੜੀ, ਨਕਲੀ ਸਿਮ ਅਤੇ ਫਰਾਡ ਕਾਲਾਂ ਵਰਗੀਆਂ ਸਮੱਸਿਆਵਾਂ ਨੂੰ ਰੋਕਣ ਵਿੱਚ ਅਹਿਮ ਭੂਮਿਕਾ ਨਿਭਾਂਦੀ ਹੈ।

19. ਆਪਣਾ ਮੋਬਾਈਲ ਫੋਨ ਹੈਕਿੰਗ ਤੋਂ ਕਿਵੇਂ ਸੁਰੱਖਿਅਤ ਰੱਖੀਏ

ਅੱਜ ਦੇ ਡਿਜੀਟਲ ਯੁੱਗ ਵਿੱਚ ਮੋਬਾਈਲ ਫੋਨ ਸਿਰਫ਼ ਗੱਲ ਕਰਨ ਦਾ ਸਾਧਨ ਨਹੀਂ ਰਹਿ ਗਿਆ, ਸਗੋਂ ਇਹ ਸਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ, ਬੈਂਕਿੰਗ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਦਫ਼ਤਰੀ ਕੰਮਾਂ ਦਾ ਮਹੱਤਵਪੂਰਨ ਹਿੱਸਾ ਬਣ ਚੁੱਕਾ ਹੈ। ਇਸ ਕਰਕੇ ਮੋਬਾਈਲ ਦੀ ਸੁਰੱਖਿਆ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਜੇਕਰ ਮੋਬਾਈਲ ਹੈਕ ਹੋ ਜਾਵੇ ਤਾਂ ਪੈਸਿਆਂ ਦਾ ਨੁਕਸਾਨ, ਨਿੱਜਤਾ ਭੰਗ ਅਤੇ ਡਾਟਾ ਚੋਰੀ ਵਰਗੀਆਂ ਸਮੱਸਿਆਵਾਂ ਪੈਦਾ ਹੋ ਸਕਦੀਆਂ ਹਨ।

1. ਮੋਬਾਈਲ ਵਿੱਚ ਮਜ਼ਬੂਤ ਸਕ੍ਰੀਨ ਲੋਕ ਲਗਾਉਣਾ ਚਾਹੀਦਾ ਹੈ। ਪਿਨ, ਪੈਟਰਨ ਜਾਂ ਪਾਸਵਰਡ ਸੈੱਖਾ ਨਾ ਹੋਵੇ। ਬਾਇਓਮੈਟ੍ਰਿਕ ਲੋਕ (ਫਿੰਗਰਪ੍ਰਿੰਟ ਜਾਂ ਫੇਸ ਲੋਕ) ਦੀ ਵਰਤੋਂ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ ਅਤੇ ਸਕ੍ਰੀਨ ਲੋਕ ਆਟੋ-ਟਾਈਮ ਘੱਟ ਰੱਖਣਾ ਚਾਹੀਦਾ ਹੈ।
2. ਸਿਰਫ਼ ਭਰੋਸੇਯੋਗ ਐਪਸ ਹੀ ਡਾਊਨਲੋਡ ਕਰੋ। ਐਪ ਹਮੇਸ਼ਾ **Google Play Store** ਜਾਂ **Apple App Store** ਤੋਂ ਹੀ ਇੰਸਟਾਲ ਕਰੋ। ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਵੈੱਬਸਾਈਟ ਜਾਂ ਲਿੰਕ ਤੋਂ **APK** ਫਾਈਲ ਡਾਊਨਲੋਡ ਕਰਨ ਤੋਂ ਬਚੋ, ਕਿਉਂਕਿ ਅਜਿਹੀਆਂ ਐਪਸ ਵਿੱਚ ਮਾਲਵੇਅਰ ਹੋ ਸਕਦਾ ਹੈ।
3. ਐਪ ਪਰਮੀਸ਼ਨਾਂ 'ਤੇ ਧਿਆਨ ਦਿਓ। ਕਈ ਐਪਸ ਬਿਨਾਂ ਲੋੜ ਦੇ ਕੈਮਰਾ, ਮਾਈਕ, ਕਾਂਟੈਕਟਸ ਜਾਂ ਲੋਕੇਸ਼ਨ ਦੀ ਪਹੁੰਚ ਮੰਗਦੀਆਂ ਹਨ। ਅਜਿਹੀ ਪਰਮੀਸ਼ਨ ਨੂੰ ਤੁਰੰਤ ਰੱਦ ਕਰੋ। ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ **Permissions Settings** ਚੈੱਕ ਕਰਦੇ ਰਹੋ।
4. ਫੋਨ ਅਤੇ ਐਪਸ ਨੂੰ ਅਪਡੇਟ ਰੱਖੋ। **Software Update** ਵਿੱਚ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਸੁਧਾਰ ਹੁੰਦੇ ਹਨ ਜੋ ਹੈਕਿੰਗ ਤੋਂ ਬਚਾਉਂਦੇ ਹਨ। ਪੁਰਾਣਾ ਸਾਫਟਵੇਅਰ ਫੋਨ ਨੂੰ ਖ਼ਤਰੇ ਵਿੱਚ ਪਾ ਸਕਦਾ ਹੈ।
5. **Public Wi-Fi** ਦੀ ਵਰਤੋਂ ਸਮੇਂ ਸਾਵਧਾਨ ਰਹੋ। ਮੁਫ਼ਤ **Wi-Fi** 'ਤੇ ਬੈਂਕਿੰਗ, ਪਾਸਵਰਡ ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰੋ। ਸੰਭਵ ਹੋਵੇ ਤਾਂ **VPN** ਦੀ ਵਰਤੋਂ ਕਰੋ।

6. **OTP, PIN** ਅਤੇ ਪਾਸਵਰਡ ਕਿਸੇ ਨਾਲ ਵੀ ਸਾਂਝੇ ਨਾ ਕਰੋ। ਕੋਈ ਵੀ ਬੈਂਕ, ਸਰਕਾਰੀ ਸੰਸਥਾ ਜਾਂ ਕੰਪਨੀ ਕਦੇ ਵੀ ਫੋਨ 'ਤੇ **OTP** ਨਹੀਂ ਮੰਗਦੀ। ਸ਼ੱਕੀ ਕਾਲ ਜਾਂ ਮੈਸੇਜ ਤੋਂ ਤੁਰੰਤ ਦੂਰ ਰਹੋ।
7. ਐਂਟੀਵਾਇਰਸ ਜਾਂ ਮੋਬਾਈਲ ਸੁਰੱਖਿਆ ਐਪ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਇਹ ਐਪਸ ਮਾਲਵੇਅਰ, ਫ਼ਰਾਡ ਅਤੇ ਖ਼ਤਰਨਾਕ ਲਿੰਕਾਂ ਤੋਂ ਸੁਰੱਖਿਆ ਦਿੰਦੀਆਂ ਹਨ।
8. ਕਲਿੱਕ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚੋ। ਅਣਜਾਣ ਲਿੰਕ, ਇਨਾਮ ਜਾਂ ਲਾਟਰੀ ਵਾਲੇ ਮੈਸੇਜ ਅਕਸਰ ਧੋਖਾਧੜੀ ਹੁੰਦੇ ਹਨ। ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ।

ਅਖੀਰ ਵਿੱਚ, ਡਾਟਾ ਬੈਕਅੱਪ ਰੱਖਣਾ ਵੀ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ। ਜੇਕਰ ਕਦੇ ਫੋਨ ਹੈਕ ਜਾਂ ਗੁੰਮ ਹੋ ਜਾਵੇ, ਤਾਂ ਡਾਟਾ ਸੁਰੱਖਿਅਤ ਰਹੇਗਾ।

ਮੋਬਾਈਲ ਸੁਰੱਖਿਆ ਸਾਡੀ ਆਪਣੀ ਜ਼ਿੰਮੇਵਾਰੀ ਹੈ। ਥੋੜ੍ਹੀ ਸਾਵਧਾਨੀ ਅਤੇ ਸਹੀ ਆਦਤਾਂ ਅਪਣਾ ਕੇ ਅਸੀਂ ਆਪਣੇ ਮੋਬਾਈਲ ਨੂੰ ਹੈਕਿੰਗ ਤੋਂ ਕਾਫ਼ੀ ਹੱਦ ਤੱਕ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹਾਂ। ਯਾਦ ਰੱਖੋ, ਸਾਵਧਾਨੀ ਹੀ ਸਭ ਤੋਂ ਵੱਡੀ ਸੁਰੱਖਿਆ ਹੈ।

20. ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦਾ ਪ੍ਰਣ

ਅੱਜ ਦੇ ਡਿਜੀਟਲ ਯੁੱਗ ਵਿੱਚ, ਮੈਂ _____ ਇੰਟਰਨੈੱਟ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋਏ ਹਮੇਸ਼ਾ ਆਪਣੇ ਆਪ ਨੂੰ ਸਾਈਬਰ ਖਤਰਿਆਂ ਤੋਂ ਬਚਾਉਣ ਅਤੇ ਇੰਟਰਨੈੱਟ ਦੀ ਦੁਨੀਆ ਵਿੱਚ ਸਾਈਬਰ ਨੈਤਿਕਤਾ ਦੀ ਪਾਲਣਾ ਕਰਨ ਦਾ ਪ੍ਰਣ ਲੈਂਦਾ/ਲੈਂਦੀ ਹਾਂ ਕਿ

1. ਮੈਂ, ਮੋਬਾਈਲ ਤੇ ਪ੍ਰਾਪਤ ਮੈਸੇਜ, ਈਮੇਲ, ਫੇਕ ਜਾਂ ਜਾਅਲੀ ਕਾਲਾਂ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਜਾਂ ਕਿਸੇ ਵੀ ਆਨਲਾਈਨ ਪਲੇਟਫਾਰਮ ਤੇ ਪ੍ਰਾਪਤ ਹੋਣ ਵਾਲੇ ਮੁਨਾਫ਼ੇ ਦੀਆਂ ਪੇਸ਼ਕਸ਼ਾਂ ਦੁਆਰਾ ਲਾਲਚ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ਅਤੇ ਇਹਨਾਂ ਦਾ ਸ਼ਿਕਾਰ ਹੋ ਕੇ ਕਦੇ ਵੀ ਬੈਂਕ ਵੇਰਵੇ, OTP ਜਾਂ ਕਿਸੇ ਵੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲਿਆਂ ਨਾਲ ਸਾਂਝਾ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ।
2. ਮੈਂ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਵਰਤੋਂ ਪੂਰੀ ਸਾਵਧਾਨੀ ਨਾਲ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ਅਤੇ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ।
3. ਮੈਂ, ਇੰਟਰਨੈੱਟ 'ਤੇ ਮੇਰੇ ਹਰੇਕ ਮਹੱਤਵਪੂਰਨ ਖਾਤੇ ਲਈ ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਰੱਖਾਂਗਾ/ਰੱਖਾਂਗੀ ਅਤੇ ਕਿਸੇ ਵੀ ਸਥਿਤੀ ਵਿੱਚ ਕਿਸੇ ਨਾਲ ਪਾਸਵਰਡ ਸਾਂਝਾ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ।
4. ਮੈਂ, ਮੋਬਾਈਲ ਤੇ ਪ੍ਰਾਪਤ ਮੈਸੇਜ, ਈਮੇਲ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਜਾਂ ਕਿਸੇ ਵੀ ਸਰੋਤ ਤੋਂ ਪ੍ਰਾਪਤ ਸੰਦੇਸ਼ ਜਾਂ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਕੇ ਆਪਣੇ ਮੋਬਾਈਲ 'ਤੇ ਕੋਈ ਐਪ ਇੰਸਟਾਲ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ਅਤੇ ਕੋਈ ਨਿੱਜੀ ਜਾਂ ਬੈਂਕ ਵੇਰਵੇ ਸਾਂਝੇ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ।
5. ਮੈਂ, ਆਪਣੇ ਸਾਰੇ ਬੈਂਕ ਨਾਲ ਸਬੰਧਤ ਜਾਂ ਕੋਈ ਹੋਰ ਯੂਜ਼ਰਨੇਮ ਅਤੇ ਪਾਸਵਰਡ ਆਪਣੇ ਮੋਬਾਈਲ ਜਾਂ ਕੰਪਿਊਟਰ 'ਤੇ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ਅਤੇ ਨਾ ਹੀ ਲਿਖਾਂਗਾ/ਲਿਖਾਂਗੀ ਅਤੇ ਉਹਨਾਂ ਨੂੰ ਯਾਦ ਰੱਖਣ ਦੀ ਪੂਰੀ ਕੋਸ਼ਿਸ਼ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ।
6. ਮੈਂ, ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਆਪਣੇ ਮੋਬਾਈਲ ਐਪਸ, ਮੋਬਾਈਲ ਓਪਰੇਟਿੰਗ ਸਿਸਟਮ ਅਤੇ ਕੰਪਿਊਟਰ ਸਾਫਟਵੇਅਰਾਂ ਨੂੰ ਅਪਡੇਟ ਕਰਦਾ ਰਹਾਂਗਾ/ਰਹਾਂਗੀ।

7. ਮੈਂ, ਕਦੇ ਇੰਟਰਨੈੱਟ 'ਤੇ ਬਣੇ ਦੋਸਤਾਂ ਨੂੰ ਪਹਿਲੀ ਵਾਰ ਇਕੱਲੇ ਮਿਲਣ ਨਹੀਂ ਜਾਵਾਂਗਾ/ਜਾਵਾਂਗੀ, ਜ਼ਰੂਰੀ ਹੋਇਆ ਵੀ ਤਾਂ ਮੈਂ ਇਸ ਲਈ ਆਪਣੇ ਪਰਿਵਾਰ ਦੇ ਜਿੰਮੇਵਾਰ ਮੈਂਬਰ ਨੂੰ ਨਾਲ ਲੈ ਕੇ ਜਾਵਾਂਗਾ/ਜਾਵਾਂਗੀ
8. ਮੈਂ, ਜੇਕਰ ਮੈਂ ਆਪਣੇ ਆਪ ਨੂੰ ਇੰਟਰਨੈੱਟ 'ਤੇ ਅਸੁਰੱਖਿਅਤ ਪਾਉਂਦਾ/ਪਾਉਂਦੀ ਹਾਂ ਜਾਂ ਕੋਈ ਵਿਅਕਤੀ ਮੈਨੂੰ ਇੰਟਰਨੈੱਟ 'ਤੇ ਧਮਕੀਆਂ ਦਿੰਦਾ ਹੈ, ਡਰਾਉਂਦਾ ਹੈ ਜਾਂ ਬਲੈਕਮੇਲ ਕਰਦਾ ਹੈ, ਤਾਂ ਮੈਂ ਆਪਣੇ ਪਰਿਵਾਰਕ ਮੈਂਬਰਾਂ ਨੂੰ ਇਸ ਬਾਰੇ ਦੱਸਾਂਗਾ/ ਦੱਸਾਂਗੀ ਅਤੇ ਜੇਕਰ ਲੋੜ ਪਈ ਤਾਂ ਮੈਂ ਪੁਲਿਸ ਨੂੰ ਰਿਪੋਰਟ ਕਰਾਂਗਾ/ ਕਰਾਂਗੀ ।
9. ਮੈਂ, ਖੁਦ, ਕਦੇ ਵੀ ਇੰਟਰਨੈੱਟ, ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕਿਸੇ ਕਿਸਮ ਦੀ ਪਰੇਸ਼ਾਨੀ, ਅਫਵਾਹ ਫੈਲਾਉਣ, ਦੰਗਾ ਭੜਕਾਉਣ ਵਾਲੀਆਂ ਗਤੀਵਿਧੀਆਂ ਵਿੱਚ ਸ਼ਾਮਲ ਨਹੀਂ ਹੋਵਾਂਗਾ/ਹੋਵਾਂਗੀ, ਅਤੇ ਕਦੇ ਵੀ ਇਸ ਵਿੱਚ ਸ਼ਾਮਲ ਨਹੀਂ ਹੋਵਾਂਗਾ/ ਹੋਵਾਂਗੀ ।
10. ਅੰਤ ਵਿੱਚ, ਮੈਂ ਇੱਕ ਵਾਰ ਫਿਰ ਸਹੁੰ ਚੁੱਕਦਾ/ਚੁੱਕਦੀ ਹਾਂ ਕਿ ਇੱਕ ਜਿੰਮੇਵਾਰ ਨਾਗਰਿਕ ਹੋਣ ਦੇ ਨਾਤੇ, ਮੈਂ ਆਪਣੇ ਆਪ ਨੂੰ, ਆਪਣੇ ਪਰਿਵਾਰ ਨੂੰ ਅਤੇ ਆਪਣੇ ਦੇਸ਼ ਨੂੰ ਸਾਈਬਰ ਸੁਰੱਖਿਅਤ ਰੱਖਾਂਗਾ/ ਰੱਖਾਂਗੀ, ਤਾਂ ਜੋ ਮੇਰਾ ਦੇਸ਼ ਡਿਜੀਟਲ ਸੰਸਾਰ ਵਿੱਚ ਇੱਕ ਸ਼ਕਤੀਸ਼ਾਲੀ ਤਰੀਕੇ ਨਾਲ ਅੱਗੇ ਵਧ ਸਕੇ।

ਆਪ ਸਭ ਦਾ ਧੰਨਵਾਦ ਅਤੇ ਆਸ ਕਰਦਾ ਹਾਂ ਕੀ ਇਸ ਬੁੱਕਲੈਟ ਨੂੰ ਤੁਸੀਂ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹਿਆ ਹੋਵੇਗਾ ਅਤੇ ਆਪਣੇ ਆਪ ਨੂੰ ਆਨਲਾਈਨ ਦੁਨੀਆਂ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਹਮੇਸ਼ਾ ਯਤਨਸ਼ੀਲ ਰਹੋਗੇ।

ਇਸ ਹੈਂਡਬੁੱਕ ਸਬੰਧੀ ਕਿਸੇ ਵੀ ਤਰ੍ਹਾਂ ਦੇ ਸੁਝਾਅ ਲਈ ਹੇਠ ਲਿਖੇ ਈਮੇਲ ਆਈਡੀ ਤੇ ਆਪਣੇ ਵਿਚਾਰ ਦੇ ਸਕਦੇ ਹੋ ਜੀ:

vishalwatts.fazilka@gmail.com

ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦਾ ਪ੍ਰਣ

ਮੈਂ _____ ਆਪਣੇ ਅਤੇ ਸਮਾਜ ਲਈ ਸਾਈਬਰ ਜਗਤ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਮਾਹੌਲ ਸਿਰਜਣ ਲਈ ਪ੍ਰਣ ਲੈਂਦਾ/ਲੈਂਦੀ ਹਾਂ ਕਿ

1. ਮੈਂ, ਮੋਬਾਈਲ ਤੇ ਪ੍ਰਾਪਤ ਮੈਸੇਜ, ਈਮੇਲ, ਫੇਕ ਜਾਂ ਜਾਅਲੀ ਕਾਲਾਂ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਜਾਂ ਕਿਸੇ ਵੀ ਆਨਲਾਈਨ ਪਲੇਟਫਾਰਮ ਤੇ ਪ੍ਰਾਪਤ ਹੋਣ ਵਾਲੇ ਮੁਨਾਫ਼ੇ ਦੀਆਂ ਪੇਸ਼ਕਸ਼ਾਂ ਦੁਆਰਾ ਲਾਲਚ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ਅਤੇ ਇਹਨਾਂ ਦਾ ਸ਼ਿਕਾਰ ਹੋ ਕੇ ਕਦੇ ਵੀ ਬੈਂਕ ਵੇਰਵੇ, OTP ਜਾਂ ਕਿਸੇ ਵੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲਿਆਂ ਨਾਲ ਸਾਂਝਾ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ।
2. ਮੈਂ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਦੀ ਵਰਤੋਂ ਪੂਰੀ ਸਾਵਧਾਨੀ ਨਾਲ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ਅਤੇ ਆਪਣੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ।
3. ਮੈਂ, ਇੰਟਰਨੈੱਟ 'ਤੇ ਮੇਰੇ ਹਰੇਕ ਮਹੱਤਵਪੂਰਨ ਖਾਤੇ ਲਈ ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਰੱਖਾਂਗਾ/ਰੱਖਾਂਗੀ ਅਤੇ ਕਿਸੇ ਵੀ ਸਥਿਤੀ ਵਿੱਚ ਕਿਸੇ ਨਾਲ ਪਾਸਵਰਡ ਸਾਂਝਾ ਨਹੀਂ ਕਰਾਂਗਾ/ਕਰਾਂਗੀ ।
4. ਮੈਂ, ਕਦੇ ਇੰਟਰਨੈੱਟ 'ਤੇ ਬਣੇ ਚੋਸਤਾਂ ਨੂੰ ਪਹਿਲੀ ਵਾਰ ਇਕੱਲੇ ਮਿਲਣ ਨਹੀਂ ਜਾਵਾਂਗਾ/ਜਾਵਾਂਗੀ, ਜ਼ਰੂਰੀ ਹੋਇਆ ਵੀ ਤਾਂ ਮੈਂ ਇਸ ਲਈ ਆਪਣੇ ਪਰਿਵਾਰ ਦੇ ਜ਼ਿੰਮੇਵਾਰ ਮੈਂਬਰ ਨੂੰ ਨਾਲ ਲੈ ਕੇ ਜਾਵਾਂਗਾ/ਜਾਵਾਂਗੀ ।
5. ਮੈਂ, ਜੇਕਰ ਆਪਣੇ ਆਪ ਨੂੰ ਇੰਟਰਨੈੱਟ 'ਤੇ ਅਸੁਰੱਖਿਅਤ ਪਾਉਂਦਾ/ਪਾਉਂਦੀ ਹਾਂ ਜਾਂ ਕੋਈ ਵਿਅਕਤੀ ਮੈਨੂੰ ਇੰਟਰਨੈੱਟ 'ਤੇ ਧਮਕੀਆਂ ਦਿੰਦਾ ਹੈ, ਡਰਾਉਂਦਾ ਹੈ ਜਾਂ ਬਲੈਕਮੇਲ ਕਰਦਾ ਹੈ, ਤਾਂ ਮੈਂ ਆਪਣੇ ਪਰਿਵਾਰਕ ਮੈਂਬਰਾਂ ਨੂੰ ਇਸ ਬਾਰੇ ਦੱਸਾਂਗਾ/ ਦੱਸਾਂਗੀ ਅਤੇ ਜੇਕਰ ਲੋੜ ਪਈ ਤਾਂ ਮੈਂ ਪੁਲਿਸ ਨੂੰ ਰਿਪੋਰਟ ਕਰਾਂਗਾ/ ਕਰਾਂਗੀ ।



ਕਵਰ ਪੇਜ ਤਿਆਰ ਕਰਤਾ: ਪਰਵਿੰਦਰ ਸਿੰਘ ਸੈਣੀ, ਕੰਪਿਊਟਰ ਫੈਕਲਟੀ, ਸ.ਸ.ਸ.ਸ. ਚਿਮਨੇਵਾਲਾ