தினமலர்
வாரமலர்
27.8.2023 நாளிதழுடன் இணைப்பு

உங்கள் குரல்...

பேசுவது நீங்கள் அல்ல... அச்சுறுத்தும் களவுநுட்பம்

"நேத்திக்கு ஒரு புது நம்பருல இருந்து என் மாமா பேசினார். 'என் போன்ல சார்ஜ் போச்சு. வெளியில இருக்கேன். இன்னொருத்தர் நம்பருல இருந்து கூப்பிடுறேன். அவசரமா 5 ஆயிரம் ரூபாய் வேணும். நான் சொல்ற நம்பருக்கு பணத்தை அனுப்பிவிடு'ன்னு சொன்னார். நானும் அனுப்பினேன். இன்னிக்கு அவரோட நம்பருக்கு கூப்பிட்டுப் பேசினப்ப, 'நான் எங்கே பேசினேன்? பணமும் கேட்கலையே'ன்னு சொல்றாரு. நேத்திக்கு என்கிட்ட அவர் குரலில் பேசினது யாருன்னே தெரியல..." சமீபமாக இப்படியான புலம்பல்கள் அதிகரித்து வருகின்றன. புலம்ப வைத்திருப்பது 'வாய்ஸ் குளோனிங் சைபர் அட்டாக்'.

பணத்தை திருடும் கும்பல், செயற்கை நுண்ணறிவு தொழில்நுட்பம் எனப்படும் ஏஐ உதவியுடன் புதிதாக கையில் எடுத்துள்ள ஆயுதம்தான் வாய்ஸ் குளோனிங் முறை. இத்தகைய தாக்குதல்கள் அடுத்த 6 மாதங்களில், 30 முதல் 35 சதவீதம் வரை அதிகரிக்கும் என்கிறது புள்ளிவிபரம் ஒன்று.

அறிந்த குரலுடன் பணத்தை அபகரிக்கும் இந்த தொழில்நுட்பம் குறித்து மேலதிக விபரங்கள் அறிய, 'டிஜிட்டல் செக்யூரிட்டி அசோசியேஷன் ஆப் இந்தியா' அமைப்பின் தலைவரும், சைபர் பிரிவு வழக்கறிஞருமான ராஜேந்திரனிடம் பேசினோம்.

"பிரபலங்கள் போலவே சில மிமிக்ரி கலைஞர்கள் பேசுவதைப் பார்த்திருப்பீர்கள். ஒரு நபரைப் போலவே இன்னொருவர் அச்சு அசலாக பேசுவது சிரமம். பயிற்சி தேவை. ஆனால், ஏஐ உதவியுடன், ஒருவரின் குரலை எளிதாக மிமிக்ரி செய்துவிட முடியும். அது துல்லியமாகவும் இருக்கும். உதாரணமாக உங்களிடம் இருந்து பணம் பறிக்க திட்டமிடுகிறார்கள் என்றால், அந்தக் கும்பல், உங்கள் சமூக வலைதளங்களில் நீங்கள் பதிவிட்டிருக்கும் வீடியோ, ஆடியோ பதிவுகளை எடுத்துக் கொண்டு ஏஐ உதவியுடன் 'வாய்ஸ் டேட்டாபேஸ்' உருவாக்குவார்கள். கோபத்தில், மகிழ்ச்சியில், சோகத்தில் எப்படி பேசுவீர்கள்? என்பதை ஏஐ தொழில்நுட்பத்தின் உதவியுடன் ஆய்வு செய்து இந்த டேட்டாபேசை உருவாக்குவார்கள்.

பின்னர் இதை வைத்து பணம் பறிக்கும் வேலையில் இறங்குவார்கள். உங்கள் உறவினர்கள், நண்பர்களுக்கு போன் செய்து, உங்கள் குரலில் பணம் கேட்பார்கள். உங்கள் குரலில் பணம் கேட்கும்போது எதிர்முனையில் இருப்பவர் நம்பிவிடுவார் என்பதால் இது சமீபமாக அதிகளவில் நடந்துவருகிறது" என்று இந்த 'களவு'நுட்பத்தின் செயல்பாடு பற்றி விளக்கம் கொடுக்கும் ராஜேந்திரன், 8 ஆண்டுகளுக்கு முன்பே வங்கிகளில் எவ்வாறெல்லாம் இணைய வழி தாக்குதல்கள் நடக்கக்கூடும் என்பது தொடர்பாக புத்தகம் எழுதியிருக்கிறார். அந்தப் புத்தகத்தில் 'வாய்ஸ் குளோனிங் சைபர் அட்டாக்' பற்றியும் குறிப்பிட்டிருக்கிறார்.

ராஜேந்திரன்

"அன்று நான் கணித்தது, இன்று நிஜமாகியிருக்கிறது. வங்கியை தொடர்புகொள்ளும் போது, உங்களுக்குத் தேவையான சேவைகளை, தொலைபேசி வழியாக நீங்கள் கொடுக்கும் உத்திரவாதத்தின் அடிப்படையில் அவர்கள் செய்து கொடுக்கிறார்கள்.

நீங்கள் பேசுவது பதிவு செய்யப்பட்டு, ஆவணமாக்கப்படும். குரல் பதிவானது ஒரு 'எலக்ட்ரானிக் ஆவணம்' என்று சொல்கிறது தொழில்நுட்பச் சட்டம். ஒரு காகிதத்தில் கையெழுத்து போட்டு, அதை ஆவணமாக மாற்றுவதைப் போல, குரல் வழியாக நீங்கள் கொடுக்கும் உத்திரவாதமும், பதிவு செய்யப்பட்டு ஆவணமாக்கப் படும். இந்த முறை மிகவும் ஆபத்தானது" என்றவர், தொடர்ந்தார்.

"தொழில்நுட்பத்தின் வளர்ச்சியையும், அதனால் ஏற்படும் அபாயங்களையும் தடுக்க முடியாது. தொழில்நுட்பத்தை தடை செய்யவும் முடியாது. அதனால், அதன் வளர்ச்சிக்கு இணையாக, பாதுகாப்பு நடவடிக்கைகளை அதிகரிக்க வேண்டும். இதற்கான முதல் தேவை மக்களிடையே இதுகுறித்த விழிப்புணர்வு. அடுத்து, சேவை நிறுவனங்களான வங்கிகள், சைபர் அட்டாக் ஏற்படாத வகையில் போதிய பாதுகாப்பு வசதிகளை செய்ய வேண்டும். மூன்றாவதாக அரசாங்கமும், நீதிமன்றங்களும், சைபர் அட்டாக் தொடர்பாக கடுமையான நடவடிக்கைகளை எடுக்க வேண்டும். அப்போது தான் இப்போது உருவெடுத்து அதிகரித்துவரும் 'வாய்ஸ் குளோனிங் சைபர் அட்டாக்' போன்றவற்றை தடுக்க முடியும் என்று முடித்தார் ராஜேந்திரன்.

உங்கள் குரலில் உங்களுக்கே வேட்டு வைக்கும் இந்த களவுநுட்பம் குறித்து உஷாரா இருங்க மக்களே!

- எம். கணேஷ்

இளைஞர்களே இலக்கு

வாய்ஸ் குளோனிங் சைபர் அட்டாக் பெரும்பாலும் இளைஞர்களை குறிவைத்தே நடத்தப்படுகிறது. சமூக வலைதளங்களைப் பயன்படுத்தும் இளைஞர்களில் 53 சதவீதம் பேர், ஆடியோ, வீடியோ என்று ஏதோ ஒரு வகையில் தங்கள் குரலை வாரம் ஒருமுறை தங்களின் சமூக வலைதளப்பக்கத்தில் பதிவிடுவதாக சொல்கிறது ஒரு புள்ளிவிபரம். வெறும் 3 வினாடிகள் கொண்ட ஆடியோவை வைத்து, ஏஐ தொழில்நுட்பத்தால் உங்கள் குரலை உருவாக்க முடியும் என்று அதிர வைக்கிறது அந்தப் புள்ளிவிபரம்.