Community Resilience to Foreign Interference

National Cyber Security Centre

உங்கள் நிறுவனத்தை ஆன்லைனில் பாதுகாப்பாக வைத்திருத்தல்

சமூகக் குழுக்கள் மற்றும் நிறுவனங்களுக்கு இணையப் பாதுகாப்பு ஏன் முக்கியமானது?

இந்தப் பக்கத்தில் இணையப் பாதுகாப்பு அச்சுறுத்தல்களிலிருந்து உங்கள் சமூகக் குழு அல்லது நிறுவனத்தைப் பாதுகாக்க ஆலோசனையும் சில நடவடிக்கைகளும் உள்ளன. தனிநபர்கள் தங்களை ஆன்லைனில் பாதுகாப்பாக வைத்திருக்க தனி வழிகாட்டியும் உள்ளது.

இந்த ஆலோசனை மிகவும் பொதுவான மற்றும் தீவிரமான அச்சுறுத்தல்களை அடிப்படையாகக் கொண்டது.

புதுப்பிப்புகள்

பாதுகாப்பில் ஏதாவது குறைபாடு இருந்தால் சரி செய்ய உங்கள் சாதனங்களில் மென்பொருளைப் புதுப்பித்த நிலையில் வைத்திருங்கள்.

- உங்கள் சமூகக் குழு அல்லது நிறுவனத்தின் சாதனங்களைப் புதுப்பித்த நிலையில் வைத்திருங்கள். இதில் தொலைபேசிகள், கணினிகள், வைஃபை (WiFi) திசைவிகள் மற்றும் எதுவாயினும் இணையத்துடன் இணைக்கும் அனைத்தும் அடங்கும் - ஸ்மார்ட் சாதனங்கள் உட்பட.
- சாத்தியமான இடங்களில் தானியங்கி புதுப்பிப்புகளைப் பயன்படுத்தவும்.

இரண்டு காரணி உறுதிப்படுத்துதல் (2FA)

கடவுச்சொல் மற்றும் உங்கள் தொலைபேசியில் உள்ள செயலியில் இருக்கும் குறியீடு போன்ற இன்னும் ஒரு படி தேவைப்படுவதன் மூலம் உங்கள் கணக்குகளுக்கு கூடுதல் பாதுகாப்பைச் சேர்க்கிறது.

- குறிப்பு: இது பல காரணி உறுதிப்படுத்துதல் (MFA), இரண்டு படி சரிபார்ப்பு (2SV) மற்றும் பல பெயர்களால் அழைக்கப்படுகிறது.
- உங்கள் சமூகக் குழு அல்லது நிறுவனத்தின் கணக்குகள் அனைத்திலும் 2FA -ஐ ஆன் செய்யவும்.
- முடிந்தால், ஃபிஷிங் (இணையதள ஏமாற்றம்) எதிர்ப்பு கொண்ட 2FA படிவத்தை பயன்படுத்த முயற்சிக்கவும், அதாவது தகவல்களை உங்களிடம் இருந்து ஏமாற்றி எடுக்க முடியாது. இது பிசிக்கல் செக்யூரிட்டி கீ அல்லது கைரேகை அல்லது ஃபேஸ் ஐடி போன்றதாக இருக்கலாம்.

உங்கள் ஆன்லைன் கணக்குகளைக் கண்காணிக்கவும்

சமூகக் குழு அல்லது நிறுவனத்தை விட்டு வெளியேறிய பிறகு முன்னாள் உறுப்பினர்கள் கணக்குகளுக்கான அணுகலைத் தொடரவில்லை என்பதை உறுதிப்படுத்தவும்.

- ஒரு கணக்கை ஒன்றுக்கு மேற்பட்டவர்கள் அணுகினால், அவர்கள் அனைவருக்கும் வெவ்வேறு உள்நுழைவுகள் இருப்பதை உறுதிசெய்து, அனைவருக்கும் 2FA ஆன் செய்யப்பட்டுள்ளது என்று உறுதிப்படுத்திக் கொள்ளுங்கள்.
- அனைத்து பயனர் கணக்குகளின் பட்டியலை வைத்து, ஊழியர்கள் வெளியேறும் போது தேவையில்லாதவற்றை செயலிழக்கச் செய்யவும்.
- உங்கள் உறுப்பினர்களுக்கு நீங்கள் வழங்கிய சாதனங்களின் பதிவேட்டை வைத்து, அந்த நபர் நிறுவனத்தை விட்டு வெளியேறினால், அவற்றைத் திரும்பப் பெற்று ஃபேக்டரி ரீசெட் செய்யவும். கட்டிட அணுகலுக்கான குறியீடுகளையும் நீங்கள் மாற்ற வேண்டியிருக்கும்.

உங்கள் ஆன்லைன் கணக்குகளுக்கான அணுகல் யாரிடம் உள்ளது என்பதைச் சரிபார்க்கவும்

உங்கள் சமூகக் குழு அல்லது நிறுவனத்தில் உள்ளவர்கள் அவர்களுக்குத் தேவையானவற்றை மட்டுமே அணுக வேண்டும்.

- ஒரு நபரின் கணக்கு ஹேக் செய்யப்பட்டால், இந்த படிகள், தாக்குபவர் செய்யக்கூடிய தீங்கைக் கட்டுப்படுத்துகின்றன.
- தேவையற்ற அனுமதிகளை அவ்வப்போது சரிபார்த்து அகற்றவும்.
- பல நபர்கள் பயன்படுத்தும் ஒற்றை "நிர்வாகி" கணக்கு உங்களிடம் இருந்தால், அசாதாரண செயல்பாட்டிற்காக அதைக் கண்காணிக்கவும். இந்த வகையான கணக்குகளை வைத்திருப்பதை மட்டுப்படுத்த முயற்சிக்கவும், குறிப்பாக அன்றாட பணிகளுக்கு.
- திசைவிகள் போன்ற சாதனங்களுக்கான நிர்வாகி அணுகலுக்கும் இந்த விதிகள் பொருந்தும்.

உங்களுக்காக IT சேவைகளை இயக்க நீங்கள் யாரையாவது பணியமர்த்தியிருந்தால்

சேவை வழங்குநர்களுடனான உங்கள் ஒப்பந்தங்களை மதிப்பாய்வு செய்யுங்கள்.

- உங்கள் சமூகக் குழு அல்லது நிறுவனத்தின் தேவைகளைப் பூர்த்தி செய்ய அவர்களிடம் இணையப் பாதுகாப்புத் தடுப்பான்கள் இருப்பதை உறுதிப்படுத்திக் கொள்ளுங்கள்.

உங்கள் கணக்குகள் மற்றும் அமைப்புகள் அனைத்தும் எவ்வாறு ஒன்றிணைந்து செயல்படுகின்றன என்பதை அறிந்து கொள்ளுங்கள்

இணைப்புகளைப் புரிந்துகொள்வது, தாக்குபவர் எங்கு நுழைய முடியும் என்பதை அறிய உதவுகிறது.

- உங்கள் கணினிகளுக்கு இடையே உள்ள இணைப்புகளை மதிப்பாய்வு செய்யவும், எடுத்துக்காட்டாக, மின்னஞ்சல், கிளவுட் ஸ்டோரேஜ் மற்றும் கணக்கியல் தளங்கள்.

- கூடுதல் ஆன்லைன் பாதுகாப்பிற்காக விர்ச்சுவல் பிரைவேட் நெட்வொர்க்கை (VPN) பயன்படுத்தவும். VPN-ஐப் பயன்படுத்துவது உங்களைக் கண்காணிக்க முயற்சிக்கும் எவரிடமிருந்தும் உங்கள் ஆன்லைன் செயல்பாட்டை மறைக்கிறது. உங்கள் சமூகக் குழு அல்லது அமைப்பின் எந்தவொரு உறுப்பினர்களும் தொலைதூரத்தில் இருந்து இணைந்தால் இது மிகவும் நல்லது.

உங்கள் மக்களை 'சைபர் ஸ்மார்ட்டாக' வைத்திருங்கள்

உங்கள் அமைப்புகளை விட உங்கள் சமூகக் குழு அல்லது நிறுவனத்தில் உள்ளவர்கள் குறிவைக்கப்படுவதற்கான வாய்ப்புகள் அதிகம்.

- அடிப்படை இணைய பாதுகாப்பில் அனைத்து ஊழியர்களுக்கும் பயிற்சி அளிக்கவும். உங்களுடைய ஆன்லைனை உங்களுடையதாக்குங்கள் இணையதளம் Own Your Online | NCSC கொண்டுள்ளது ஆன்லைனில் உங்களைப் பாதுகாப்பாக வைத்திருக்கவும், மோசடிகளைக் கண்டறிவதற்கான பரந்த அளவிலான ஆலோசனைகள் மற்றும் உதவிக்குறிப்புகளையும் கொண்டுள்ளது.
- இது அவர்களின் தனிப்பட்ட கணக்குகளுக்கும் உங்கள் நிறுவனத்திற்கு அவர்கள் பயன்படுத்தும் கணக்குகளுக்கும் முக்கியமானது என்பதை அவர்களுக்கு நினைவூட்டுங்கள்.
- தனிநபர்கள் தங்களை ஆன்லைனில் பாதுகாப்பாக வைத்திருப்பதற்கான வழிகாட்டி எங்களிடம் உள்ளது.

ஒரு நிகழ்விற்கான திட்டமிடல்

ஒரு நிகழ்வு நிகழும்போது மக்கள் பீதியடைவதைத் தடுக்க ஒரு பதிலளிப்புத் திட்டத்தை வைத்திருப்பது முக்கியம்.

- ஒரு நிகழ்வின் போது யார் என்ன செய்கிறார்கள் என்பதை ஒரு நிகழ்வு பதிலளிப்பு திட்டம் கோடிட்டுக் காட்டுகிறது. டெம்ப்ளேட்டுகள் இங்கே கிடைக்கின்றன Incident Management |NCSC
- தொலைபேசிகள், கணினிகள் அல்லது பிற அமைப்புகளில் குறைபாடு ஏற்பட்டால் என்ன செய்வது என்பதற்கான திட்டத்தைச் சேர்க்கவும். இந்த திட்டத்தை புதுப்பித்து வைத்திருங்கள்.

- ஒருவேளை அவர்களைத் தொடர்பு கொள்வதற்கான முக்கிய வழி ((மின்னஞ்சல் போன்றவை)) செயலற்று இருந்தால், தேவையான அனைவரின் தொடர்பு விவரங்களையும், காப்புப் பிரதி விவரங்களையும் வைத்திருங்கள் .
- நீங்கள் அதைப் பெற முடியாவிட்டால், திட்டத்தை உங்கள் கணினிக்கு வெளியே எங்காவது வைத்திருங்கள்.