للنشر فورًا: 22/3/2022 **الحاكمة كاثي هوكول**

الحاكمة هوكول تحذر المستهلكين بشأن عمليات الاحتيال وتهديدات الأمن السيبراني وسط الغزو الروسي لأوكرانيا

تبرع للمنظمات التي تم التحقق منها وذات السمعة الطيبة التي تستخدم المساهمات لتقديم الإغاثة إلى الأوكرانيين المحتاجين

تصدر وكالات الولاية توصيات لحماية معلوماتك الحساسة وتأمينها والبقاء في حالة تأهب تحت التهديدات الإلكترونية المتزايدة

نصحت الحاكمة كاثي هوكول سكان نيويورك اليوم بشأن عمليات الاحتيال الخيرية وتهديدات الأمن السيبراني المتزايدة المتعلقة بغزو فلاديمير بوتين لأوكرانيا. علم قسم حماية المستهلك في ولاية نيويورك بطلبات احتيالية لأموال الإغاثة الخيرية لدعم ضحايا الحرب. يتم تشجيع المستهلكين على تقييم أي طلب للحصول على المال بعناية والتحقق من المؤسسات الخيرية قبل التبرع بالمال أو الإمدادات. تشجع الحاكمة هوكول أيضًا سكان نيويورك على البقاء على أهبة الاستعداد عند إصدار معلومات حساسة عبر الإنترنت وسط تصاعد في تهديدات الأمن السيبراني من خلال استخدام التوصيات الأمنية من إدارة الضرائب والمالية. ويأتي هذا بعد تشكيل الحاكمة مركز العمليات الأمنية المشتركة والذي يعمل كمركز لمركز عمليات مشتركة على المستوى المحلي والولائي والفيدرالي لجهود الأمن السيبراني.

قالت الحاكمة هوكول، "نيويورك هي موطن لأكبر عدد من الأوكرانيين في الولايات المتحدة وسكان نيويورك دائمًا يقدمون يد العون لرعاية المحتاجين." "ومع ذلك، يجب أن نتوخى الحذر تجاه أولئك الذين يحاولون ارتكاب الاحتيال مستغلين لطف الآخرين. تذكر، في كرمك لمساعدة أصدقائنا وعائلتنا الأوكرانيين، إذا كان هناك شيء يبدو مريبًا فمن المحتمل أن يكون مريباً بالفعل. شجع أصدقائك وعائلتك وخاصة أحباءك المسنين على البقاء يقظين على الإنترنت."

في أي وقت تحدث فيه الكوارث ينقض المحتالون على قلوب الأفراد الذين يتطلعون إلى المساعدة. يوفر غزو أوكرانيا فرصة للمحتالين لتأسيس جمعيات خيرية مزيفة أو الظهور كضحايا حرب مقنعين. يصمم آخرون مواقع إلكترونية لتقليد الموقع الرسمي لمؤسسة خيرية لسرقة أموال المتبرعين المطمئنين و/أو معلوماتهم الشخصية.

قال روبرت جيه رودريغيز سكرتير الخدمات العامة، "يُعرف سكان نيويورك بأنهم يدعمون المحتاجين بسخاء. مع احتدام الحرب في أوكرانيا سيستمر المحتالون في الظهور باستخدام الحيل العاطفية والطلبات الزائفة في محاولة لإغراء المستهلكين. أنا أشجع سكان نيويورك على حماية نواياهم الحسنة والبحث دائمًا عن مؤسسة خيرية قبل التبرع للتأكد من وصول الأموال التي جمعتها بشق الأنفس إلى أولئك الذين هم في أمس الحاجة إلى دعمكم."

قالت أماندا هيلر المفوضة بالوكالة لشؤون الضرائب والتمويل، "لقد أدت الأزمة العالمية في أوكرانيا إلى تكثيف القلق بشأن الهجمات الإلكترونية لذلك يجب علينا جميعًا توخي الحذر لمنع وقوع المعلومات السرية في الأيدي الخطأ وهجمات رفض تقديم الخدمات وعواقب سلبية أخرى."

قال رئيس قسم المعلومات في مكتب خدمات تكنولوجيا المعلومات أنجلو "توني" ريديك، "لقد تبرع عدد لا يحصى من سكان نيويورك بأحسن النوايا للجمعيات الخيرية لدعم شعب أوكرانيا وهم يحدثون فرقًا. ولكن ولسوء الحظ، فإن هذا الكرم

يخلق أيضًا فرصًا جديدة لمجرمي الإنترنت لاستغلالها. لحماية نفسك ولضمان وصول تبرعك السخي دائمًا إلى أيدي أولئك الذين يحتاجون حقًا إلى المساعدة تطلب خدمات تكنولوجيا المعلومات (Information Technology Services, ITS) من سكان نيويورك اتباع أفضل الممارسات هذه والبقاء متيقظين في ضوء التهديدات وعمليات الاحتيال عبر الإنترنت الأخيرة."

قال جاكي براي، مفوض قسم الأمن الداخلي وخدمات الطوارئ، "كل واحد من سكان نيويورك لديه دور يلعبه عندما يتعلق الأمر بتأمين معلوماتهم الشخصية وحماية أنفسهم من التهديدات الإلكترونية. نحن نعلم أنه في أوقات الحاجة يتطلع الأشخاص السيئون للاستفادة من أولئك الذين يحاولون المساعدة. إذا كنت تحاول دعم شعب أوكرانيا من خلال التبرعات عبر الإنترنت أو عبر التبرعات الرقمية فابق يقظًا واتبع أفضل الممارسات هذه للتأكد من صحة تبرعاتك والحفاظ على أمان معلوماتك."

قال عضو مجلس الشيوخ كيفن توماس، "من الواضح للعيان أن العديد من سكان نيويورك قد اتخذوا إجراءات لمساعدة الشعب الأوكراني. ولسوء الحظ، فقد كانت هناك فرصة كبيرة للمحتالين لاستغلال هذه الأزمة لتحقيق مكاسب شخصية. إنني أحث سكان نيويورك على توخي اليقظة واتخاذ احتياطات إضافية للتأكد من أن مساهماتهم السخية تذهب إلى قضايا مشروعة."

قالت عضوة الجمعية نيلي روزيتش، "يحاول المحتالون طرقًا جديدة لخداعك طوال الوقت حتى أثناء وجود أزمة دولية. بينما يجتمع سكان نيويورك معًا لدعم أوكرانيا في وقت الحاجة فمن الأهمية بمكان أن يتسلح المستهلكون بالمهارات والمعرفة لضمان عدم استغلال كرمهم. أنا ممتن للحاكمة هوكول لضمان عدم تعرض سكان نيويورك للخداع بسبب لطفهم."

غالبًا ما يجري المحتالون اتصالات عبر وسائل التواصل الاجتماعي أو رسائل البريد الإلكتروني غير المرغوب فيها أو المكالمات الهاتفية أو الرسائل النصية. قد يطلبون إرسال الأموال من خلال تطبيق دفع مثل كاش أب أو فينمو أو زيلي أو تحويل الأموال إلى حساب مصرفي خارجي أو إرسال بطاقات هدايا مدفوعة مسبقًا. تتضمن العديد من عمليات الاحتيال الأخيرة طلبات تبرعات بعملة مشفرة مثل بتكوين أو إثيريوم. فنانو الخداع مبدعون وسيستمرون في التفكير في طرق جديدة للاحتيال على الناس لذلك يجب على المستهلكين توخي الحذر دائمًا.

لمنع وقوع أموال التبرعات في الأيدي الخطأ يوصي قسم حماية المستهلك بولاية نيويورك باتخاذ الاحتياطات التالية:

- **تحقق من صحة الطلب.** يتظاهر المحتالون في كثير من الأحيان بأنهم أصدقاء أو لديهم اهتمامات عائلية أو رومانسية على وسائل التواصل الاجتماعي ويطلبون التبرعات؛ من السهل نسخ صورة شخص آخر ومعلومات عن سيرته الذاتية وإنشاء حساب مزيف باسمه على الإنترنت. إذا تلقيت طلبًا غير مرغوب فيه لتقديم الإغاثة عبر التبرعات على الإنترنت، حتى إذا بدا أنه شخص تعرفه فاتصل بهذا الشخص مباشرةً من خلال رابط اتصال مختلف للتحقق من الطلب. لا تنقر على أي روابط أو تكمل النماذج قبل التحقق من المصدر. إذا كان الطلب واردًا من شخص قابلته مؤخرًا عبر الإنترنت، فمن المرجح أنه عملية احتيال ويجب أن تكون حذرًا بشكل خاص.
- **ابحث عن المؤسسة الخيرية.** لا تعتمد على الموقع الخيري وحده. ابحث عن موقع الإنترنت قبل التبرع لأي مؤسسة خيرية باستخدام اسم المجموعة بالإضافة إلى مصطلحات البحث مثل "مراجعة" و "احتيال". توصي لجنة التجارة الفيدرالية بالتحقق من give.orgأو charitywatch.org،charitynavigator.org أو candid.org للاطلاع على تقارير وتقييمات المؤسسات الخيرية. يمكنك أيضًا التحقق من خلال خدمات الإيرادات الداخلية (Internal Revenue Service, IRS) للتحقق من أن المؤسسة الخيرية مسجلة. كما يوصي مكتب المدعي العام بمراجعة سجل الجمعيات الخيرية للاطلاع على التقارير المالية قبل التبرع للتأكد من أن المؤسسة الخيرية سليمة من الناحية المالية.
- **مقاومة تكتيكات الضغط المرتفع.** على الرغم من أن الموقف عاجل، يجب على المستهلكين مقاومة الضغط عليهم للتبرع على الفور. غالبًا ما يضغط المحتالون عليك للتبرع على الفور مما يجعلك تتجاهل علامات التحذير في القصص التي يسردونها. احذر من رسائل البريد الإلكتروني المباشرة من "الضحايا" والمحامين الذين يستخدمون قصصًا مؤلمة ويصرون على التبرع على الفور. لا تعطي المال عبر الهاتف إلى المسوقين عبر الهاتف غير

المرغوب فيهم؛ وبدلاً من ذلك، اطلب من المتصل إرسال مواد مكتوبة حول المؤسسة الخيرية ومكان التبرع إذا اخترت ذلك.

- **حافظ على خصوصية المعلومات الشخصية.** لا تعطي أبدًا رقم الضمان الاجتماعي أو بطاقة الائتمان أو رقم بطاقة الخصم أو معلومات التعريف الشخصية الأخرى ردًا على طلب خيري غير مرغوب فيه. إذا كنت ستتبرع عبر الإنترنت، فتأكد من أن اتصالك بالإنترنت آمن قبل متابعة طلبات التبرع.
- **اسأل كيف سيتم إنفاق أموالك.** يريد المستهلكون أن يعرفوا أن أموالهم تذهب مباشرة إلى الضحايا. يجب أن تكون المؤسسة الخيرية الحقيقية قادرة على إخبارك بمقدار تبرعك الذي سيذهب مباشرةً إلى البرنامج بدلاً من الرسوم الإدارية.

- **تبرع بواسطة شيك أو بطاقة ائتمان.** لا تعطي المال أبدًا باستخدام النقود أو بطاقات الهدايا أو العملات المشفرة أو أي عطاء يصعب تتبعه. قدم مساهمتك بشيك أو ببطاقة ائتمان للتأكد من أن لديك سجلًا بالتبرع. قم بكتابة الشيكات للمؤسسة الخيرية وليس لفرد. إذا اخترت التبرع عبر موقع إنترنت مؤسسة خيرية فتحقق من أن موقع الإنتنرت آمن وأن جهاز الكمبيوتر الخاص بك مزود بأحدث حماية من الفيروسات.

إذا كنت تشك في مواجهتك لمحاولة احتيالية لتلقي تبرعات فيمكنك تقديم شكوى إلى قسم حماية المستهلك بولاية نيويورك على https://dos.ny.gov/file-consumer-complaint.

الخط الساخن لمساعدة المستهلك الخاص بالقسم مفتوح من الاثنين إلى الجمعة، باستثناء أيام العطلات الرسمية من الساعة 8:30 صباحًا إلى 4:30 مساءً في 1-800-697-1220. يمكنك العثور على مزيد من المعلومات والنصائح من خلال متابعة قسم حماية المستهلك على وسائل التواصل الاجتماعي على تويتر (NYSConsumerعلى) وفيسبوك (www.facebook.com/nysconsumer).

وسط تزايد القلق الدولي بشأن الأمن السيبراني، تشارك وزارة الضرائب والمالية بولاية نيويورك أيضًا سلسلة من النصائح المهمة لمساعدة دافعي الضرائب في حماية معلوماتهم الخاصة خلال موسم الضرائب وعلى مدار العام:

كن حذرًا من رسائل البريد الإلكتروني والمكالمات الهاتفية غير المرغوب فيها التي تطلب معلومات شخصية. لا تشارك أبدًا المعلومات الشخصية مثل رقم الضمان الاجتماعي الخاص بك ردًا على رسالة بريد إلكتروني أو مكالمة هاتفية غير مرغوب فيها. إذا كانت رسالة البريد الإلكتروني أو المكالمة تدعي أنها من شركة تعمل معها فاتصل بها مباشرة لتأكيد أن جهة الاتصال شرعية. غالبًا ما يستخدم المحتالون أساليب التخويف والتهديدات المتعلقة بالديون الضريبية لإقناعك بمشاركة معلوماتك الشخصية والمالية.

تأمين أجهزتك المحمولة. قم بتطبيق تحديثات البرامج التي تصحح الثغرات الأمنية المعروفة بمجرد توفرها. استخدم ميزات الأمان المضمنة في جهازك مثل رمز المرور واستخدم البرامج التي تقوم بتشفير البيانات وإزالة المحتويات عن بُعد في حالة فقد الجهاز أو سرقته.

توخ الحذر بشأن نقاط اتصال Wi-Fi. نقاط الاتصال اللاسلكية العامة ليست آمنة، مما يعني أنه من السهل على اللصوص الإلكترونيين رؤية ما تفعله على جهازك المحمول أثناء اتصالك. حدد ما تفعله على شبكة Wi-Fi العامة وتجنب تسجيل الدخول إلى حسابات حساسة.

تعرف على تطبيقاتك. قم بمراجعة تفاصيل ومواصفات التطبيق بدقة قبل تنزيله. راجع وفهم سياسة الخصوصية لكل تطبيق جوال. اعلم أن التطبيق قد يطلب الوصول إلى موقعك ومعلوماتك الشخصية.

كن حذرًا بشأن المعلومات التي تشاركها على وسائل التواصل الاجتماعي. تجنب نشر تاريخ ميلادك أو رقم هاتفك أو عنوان منزلك أو الصور التي تحدد وظيفتك أو هواياتك. أحد الأسباب: يمكن استخدام هذا النوع من المعلومات لتحديد إجابات أسئلة

الأمان المستخدمة لإعادة تعيين كلمات المرور ويجعلك هدفًا للمحتالين الذين يسعون للوصول إلى حساباتك ومعلوماتك الشخصية.

استخدم كلمات مرور قوية. قم بإنشاء كلمات مرور مختلفة لجميع حساباتك. عندما يتعلق الأمر بكلمات المرور حاول استخدام كلمة مرور مكونة من 14 حرفًا على الأقل وهي المعيار الحالي في هذا المجال. استخدم مجموعة من الأحرف (الأحرف الكبيرة والصغيرة) والأرقام والرموز. ضع في اعتبارك عبارات المرور التي تستخدم فيها الأحرف الأولى من عبارة لا تنسى لإنشاء كلمة مرور معقدة يصعب تخمينها. قم بتغيير كلمات المرور/ عبارات المرور بانتظام.

قم بتغيير أسئلة الأمان الخاصة بك. لا تستخدم نفس أسئلة الأمان على حسابات متعددة. حدد أسئلة الأمان التي لا يمكن تخمين إجاباتها أو العثور عليها من خلال البحث في وسائل التواصل الاجتماعي أو الإنترنت.

استخدم التحقق بخطوتين للوصول إلى الحسابات. لتعزيز أمان الحسابات عبر الإنترنت اطلب كلمة مرور ورمز أمان إضافي كلما أمكن ذلك للتحقق من هويتك عند تسجيل الدخول.

احذر من التصيد الاحتيالي. لا تنقر على الروابط أو تقوم بتنزيل الملفات أو تفتح المرفقات في رسائل البريد الإلكتروني الواردة من مرسلين غير معروفين. افتح المرفقات فقط عندما تتوقعها وتعرف على محتواها حتى لو كنت تعرف المرسل.

من المهم مراجعة الخطوات الضرورية بانتظام لتأمين معلوماتك الحساسة.

الإبلاغ. إذا كنت ضحية أو تعتقد أنك قد تكون ضحية لسرقة الهوية المتعلقة بالضرائب فأبلغنا على الفور. سنتعقب معلوماتك للمساعدة في الحفاظ على خصوصيتها وحمايتها. قم بزيارة الصفحة الإلكترونية التي تخص الإبلاغ عن الاحتيال والاحتيال وانتحال الشخصية.

تستخدم إدارة الضرائب التشفير المتقدم والجدران النارية وأنظمة الكشف عن التسلل والتدابير الأمنية الأخرى لحماية أنظمتنا والبيانات الحساسة ولكن يجب أيضًا على دافعي الضرائب اتباع نهج استباقي لحماية أنفسهم عبر الإنترنت.

###

تتوفر أخبار إضافية على www.governor.ny.gov
ولاية نيويورك | الغرفة التنفيذية | press.office@exec.ny.gov | 518.474.8418