Data Privacy Tips

How do I keep my data safe?

Password Tips

Safeguarding your data starts with a strong password. Creating passwords that are difficult to figure out can help you protect your privacy. Make your password strong by using a mix of letters, numbers, and symbols.

Follow these tips to enhance your passwords:

- **Length:** Aim for at least 14 characters.
- **Complexity:** Use a mix of uppercase & lowercase letters, numbers, and special characters (e.g !, ?, etc.)**.**
  - *Tip*: Use a passphrase for your password.
- **Uniqueness:** Use different passwords/passphrases for different accounts.
- **Avoid Common Phrases:** Do not use easily guessable information like "password123" or your birthdate.
- **Enable 2FA:** Two-Factor authentication adds an extra layer of security, like adding a second lock to your front door.

Phishing Scams

Phishing is when scammers try to trick you into giving them personal information, like your credit card numbers or passwords, by pretending to be someone you trust. Typically, they try this through fake emails, but they can also use text messages or phone calls. Always be vigilant!

Common Phishing Signs / Red Flags:

- **Urgent Language:** Beware of urgent request for personal information.
- **Unfamiliar Sender:** Check the sender's email address carefully.
- **Suspicious Links:** Hover over links to see the actual URL before clicking.
- **Grammar and Spelling Errors:** Legitimate organizations usually have well-written communications.
- **Unexpected Attachments:** Do not open attachments you were not expecting.

Data Privacy Tips

How do I reduce my digital footprint?

What is a digital footprint?

AKA “digital shadow,” this is the unique trail of data that a person creates using the internet. A person’s footprint consists of personal data they directly or indirectly share and includes info like: account activity (likes, interactions, etc.), browsing history, cookies, etc.

01 Limit social media accounts

The fewer accounts you have, the less personal data you leave behind. Delete old, unused, or inactive accounts, and make your active accounts private. You can also minimize exposure by limiting posts to “friends only” and by turning off location data collection.

02 Delete old email addresses

If you’re not using an old email address, delete it. Closing unused email addresses helps reduce your exposure to data breaches and cuts down on the number of ways your information can be tracked, stolen, or hacked into.

03 Create a spam email address

Create an account specifically for newsletters, promotions, or discounts, and limit any personally identifiable information (PII) you store on that email account. That way, you keep you main inbox clear of clutter and spam.

04 Operate in stealth mode

Stealth, or incognito mode, allows you to surf the web without websites and web browsers like Google Chrome, Safari, and Firefox tracking and saving your browsing activity data locally.

Consejos sobre privacidad de datos

¿Cómo mantengo mis datos protegidos?

Consejos sobre contraseñas

La protección de sus datos comienza con una contraseña segura. Crear contraseñas que sean difíciles de adivinar puede ayudarle a proteger su privacidad. Haga que su contraseña sea segura utilizando una combinación de letras, números y símbolos.

Siga estos consejos para mejorar sus contraseñas:

• **Longitud**: Intente tener al menos 14 caracteres.

• **Complejidad**: Utilice una mezcla de letras mayúsculas y minúsculas, números y caracteres especiales (p. ej., !, ?, etc.).

Consejo: Utilice una frase de contraseña para su contraseña.

• **Exclusividad**: Usar diferentes contraseñas/frases de contraseña para diferentes cuentas.

• **Evite las frases comunes**: No utilizar información fácil de adivinar como "password123" o su fecha de nacimiento.

• **Habilitar A2F**: La autenticación de dos factores añade una capa adicional de seguridad, como añadir un segundo cerrojo a su puerta principal.

Estafas Phishing

Phishing es cuando los estafadores intentan engañarlo para que les proporcione información personal, como sus números de tarjeta de crédito o contraseñas, fingiendo ser alguien en quien confía. Normalmente, lo intentan mediante correos electrónicos falsos, pero también pueden utilizar mensajes de texto o llamadas telefónicas. ¡Esté siempre alerta!

Señales comunes de phishing/señales de alerta:

• **Lenguaje urgente**: Tenga cuidado con solicitudes urgentes de información personal.

• **Remitente desconocido**: Compruebe el dirección de correo electrónico con cuidado.

• **Enlaces sospechosos**: Pase el cursor sobre los enlaces para ver la URL real antes de hacer clic.

• **Errores gramaticales y ortográficos**: Las organizaciones legítimas suelen tener comunicaciones bien escritas.

• **Adjuntos inesperados:** No abrir adjuntos que no esperaba.

Consejos sobre privacidad de datos

¿Cómo puedo reducir mi huella digital?

¿Qué es una huella digital?

Conocida como “sombra digital”. Este es el rastro único de datos que una persona crea al utilizar Internet. La huella de una persona consiste en datos personales que comparte directa o indirectamente e incluye información como: actividad de la cuenta (me gusta, interacciones, etc.), historial de navegación, cookies, etc.

01 Limitar cuentas en redes sociales

Cuantas menos cuentas tenga, menos datos personales dejará atrás. Elimine las cuentas antiguas, sin usar o inactivas y haga que sus cuentas activas sean privadas. También puede minimizar la exposición limitando las publicaciones a “solo amigos” y desactivando la recopilación de datos de ubicación.

02 Eliminar antiguas direcciones de correo electrónico

Si no está utilizando una dirección de correo electrónico antigua, elimínela. Cerrar direcciones de correo electrónico no utilizadas ayuda a reducir su exposición a filtraciones de datos y reduce el número de formas en que se puede rastrear, robar o piratear su información.

03 Crear una dirección de correo electrónico no deseado

Cree una cuenta específicamente para boletines informativos, promociones o descuentos, y limite cualquier información de identificación personal (IIP) que almacene en esa cuenta de correo electrónico. De esta forma, mantendrá su bandeja de entrada principal libre de desorden y spam.

04 Operar en modo incógnito

Stealth, o modo incógnito, le permite navegar por la web sin que sitios web ni navegadores web como Google Chrome, Safari y Firefox rastreen y guarden localmente sus datos de actividad de navegación.

គន្លឹះអំពីឯកជនភាពទិន្នន័យ

តើធ្វើយ៉ាងណាទើបខ្ញុំអាចរក្សាសុវត្ថិភាពទិន្នន័យរបស់ខ្ញុំបាន?

គន្លឹះអំពីពាក្យសម្ងាត់

ការការពារសុវត្ថិភាពទិន្នន័យរបស់អ្នកចាប់ផ្តើមដោយមានពាក្យសម្ងាត់ខ្លាំង។ ការបង្កើតពាក្យសម្ងាត់ដែលពិបាកនឹងស្មានត្រូវអាចជួយអ្នកការពារឯកជនភាពរបស់អ្នកបាន។ ធ្វើឱ្យពាក្យសម្ងាត់របស់អ្នកខ្លាំងដោយប្រើអក្សរ លេខ និងសញ្ញារួមបញ្ចូលគ្នា។

ធ្វើតាមគន្លឹះទាំងនេះ ដើម្បីបង្កើនប្រសិទ្ធភាពពាក្យសម្ងាត់របស់អ្នក៖

- **ប្រវែង៖** ដាក់ឱ្យបានយ៉ាងតិច 14 តួ។
- **ភាពស្មុគស្មាញ៖** ប្រើអក្សរធំ អក្សរតូច លេខ និងតួអក្សរពិសេសលាយបញ្ចូលគ្នា (ឧទាហរណ៍ !, ?, ជាដើម)។
  - គន្លឹះ៖ ប្រើឃ្លាសម្ងាត់សម្រាប់ពាក្យសម្ងាត់របស់អ្នក។
- **ភាពខុសប្លែកពីគេ៖** ប្រើពាក្យសម្ងាត់/ឃ្លាសម្ងាត់ខុសគ្នាសម្រាប់គណនីផ្សេងគ្នា។
- **ជៀសវាងឃ្លាសាមញ្ញៗ៖** កុំប្រើព័ត៌មានដែលងាយនឹងស្មានត្រូវដូចជា "password123" ឬថ្ងៃខែឆ្នាំកំណើតរបស់អ្នក។
- **បើក 2FA៖** ការផ្ទៀងផ្ទាត់ពីរជំហានបន្ថែមការការពារសុវត្ថិភាពមួយកម្រិតទៀត ដែលប្រៀបដូចជាការបន្ថែមសោទីពីរសម្រាប់ទ្វារមុខរបស់អ្នកដូច្នោះដែរ។

ការឆបោកដោយដាក់នុយ

ការដាក់នុយគឺនៅពេលដែលជនឆបោកព្យាយាមបញ្ឆោតឱ្យអ្នកផ្តល់ព័ត៌មានផ្ទាល់ខ្លួន ដូចជាពាក្យសម្ងាត់ ឬលេខកាតឥណទានរបស់អ្នក ដោយក្លែងអត្តសញ្ញាណជាមនុស្សដែលអ្នកទុកចិត្ត។ ជាធម្មតា ពួកគេព្យាយាមធ្វើដូច្នេះតាមរយៈអ៊ីមែលក្លែងក្លាយ ប៉ុន្តែក៏អាចប្រើសារជាអក្សរ ឬការហៅទូរសព្ទផងដែរ។ ចូរប្រុងប្រយ័ត្នជានិច្ច!

សញ្ញានៃការដាក់នុយទូទៅ / ទង់ក្រហម៖

- **ភាសាលក្ខណៈបន្ទាន់៖** ចូរប្រយ័ត្នចំពោះសំណើសុំព័ត៌មានផ្ទាល់ខ្លួនដែលមានលក្ខណៈបន្ទាន់។
- **អ្នកផ្ញើដែលមិនស្គាល់៖** ពិនិត្យមើលអាសយដ្ឋានអ៊ីមែលរបស់អ្នកផ្ញើដោយប្រុងប្រយ័ត្ន។
- **តំណគួរឱ្យសង្ស័យ៖** ដាក់ម៉ៅស៍ពីលើតំណ ដើម្បីមើល URL ពិតប្រាកដ មុននឹងចុច។
- **កំហុសវេយ្យាករណ៍ និងអក្ខរាវិរុទ្ធ៖** ជារឿយៗ អង្គភាព/ស្ថាប័នស្របច្បាប់មានការទំនាក់ទំនងដែលសរសេរបានត្រឹមត្រូវល្អ។
- **ឯកសារភ្ជាប់ដែលមិនបានរំពឹងទុក៖** កុំបើកឯកសារភ្ជាប់ដែលអ្នកមិនរំពឹងថាមានអ្នកផ្ញើមក។

គន្លឹះអំពីឯកជនភាពទិន្នន័យ

តើធ្វើយ៉ាងណាទើបខ្ញុំអាចកាត់បន្ថយដានឌីជីថលរបស់ខ្ញុំបាន?

តើអ្វីជាដានឌីជីថល?

ហៅម្យ៉ាងទៀតថា “ស្រមោលឌីជីថល” នេះគឺជាដានទិន្នន័យខុសប្លែកពីគេដែលមនុស្សម្នាក់បង្កើតដោយប្រើអ៊ីនធឺណិត។ ដានរបស់មនុស្សម្នាក់មានទិន្នន័យផ្ទាល់ខ្លួនដែលគាត់ចែករំលែកដោយផ្ទាល់ឬដោយប្រយោល ហើយរួមបញ្ចូលព័ត៌មានដូចជា៖ សកម្មភាពគណនី (ការចូលចិត្ត ការធ្វើអន្តរកម្មជាដើម) ប្រវត្តិរុករក ខូគី ។ល។

01 កាត់បន្ថយគណនីបណ្តាញសង្គម

កាលណាអ្នកមានគណនីកាន់តែតិច អ្នកក៏បន្សល់ទិន្នន័យផ្ទាល់ខ្លួនកាន់តែតិចដែរ។ គួរលុបគណនីចាស់ៗ មិនប្រើ ឬអសកម្មចោល ហើយកំណត់គណនីសកម្មរបស់អ្នកឱ្យមានលក្ខណៈឯកជន។ អ្នកក៏អាចកាត់បន្ថយហានិភ័យដោយកំណត់ការបង្ហោះឱ្យមើលឃើញដោយ “មិត្តភក្តិប៉ុណ្ណោះ” និងដោយបិទការប្រមូលទិន្នន័យទីតាំង។

02 លុបអាសយដ្ឋានអ៊ីមែលចាស់ៗ

ប្រសិនបើអ្នកមិនប្រើអាសយដ្ឋានអ៊ីមែលចាស់ទេ គួរលុបវាចោល។ ការបិទអាសយដ្ឋានអ៊ីមែលដែលមិនប្រើអាចជួយកាត់បន្ថយហានិភ័យនៃការបំពានទិន្នន័យ និងកាត់បន្ថយចំនួនវិធីដែលព័ត៌មានរបស់អ្នកអាចត្រូវបានតាមដាន លួច ឬលួចចូល។

03 បង្កើតអាសយដ្ឋានអ៊ីមែលឥតបានការ

បង្កើតគណនីដោយឡែកសម្រាប់ព្រឹត្តិបត្រ ប្រូម៉ូសិន ឬការបញ្ចុះតម្លៃ ហើយកាត់បន្ថយព័ត៌មានដែលអាចកំណត់អត្តសញ្ញាណបុគ្គល (PII) ដែលអ្នករក្សាទុកក្នុងគណនីអ៊ីមែលនោះ។ ការធ្វើបែបនេះអាចរក្សាប្រអប់ទទួលចម្បងរបស់អ្នកមិនឱ្យមានភាពរាយប៉ាយ និងសារឥតបានការ។

04 ដំណើរការជាលក្ខណៈសម្ងាត់

មុខងារសម្ងាត់ ឬមុខងារឯកជនអាចឱ្យអ្នករុករកលើអ៊ីនធឺណិតដោយមិនឱ្យគេហទំព័រ ឬកម្មវិធីរុករកលើអ៊ីនធឺណិតដូចជា Google Chrome, Safari និង Firefox តាមដាន និងរក្សាទុកទិន្នន័យអំពីសកម្មភាពរុករករបស់អ្នកក្នុងឧបករណ៍បានឡើយ។

TECHNOLOGY & INNOVATION LONGBEACH

SMART CITY LB

សម្រាប់ព័ត៌មានបន្ថែម សូមចូលទៅកាន់
longbeach.gov/smartcity

Mga Tip sa Privacy ng Datos

Paano ko pananatilihing ligtas ang aking datos?

Mga Tip sa Password

Sa isang matibay na password nagsisimula ang pag-iingat sa iyong datos. Ang paggawa ng mga password na mahirap hulaan ay makatutulong sa iyo upang protektahan ang iyong privacy. Upang mapatibay ang iyong password, gumamit ng magkakahalong titik, numero, at simbolo.

Sundin ang mga tip na ito upang mapahusay ang iyong mga password:

- **Haba:** Paabutin ito hanggang sa hindi bababa sa 14 na karakter.
- **Pagiging Kumplikado:** Gumamit ng magkakahalong malalaki at maliliit na titik, numero, at espesyal na karakter (halimbawa, !, ?, atbp.)**.**
  - *Tip*: Gumamit ng passphrase para sa iyong password.
- **Pagiging Natatangi:** Gumamit ng magkakaibang password/passphrase para sa iba-ibang account.
- **Iwasan ang mga Karaniwang Parirala:** Huwag gumamit ng madaling hulaang impormasyon tulad ng "password123" o petsa ng iyong kapanganakan.
- **I-enable ang 2FA:** Nakadaragdag ang Two-Factor Authentication (Pagpapatotoong may Dalawang Salik) ng ekstrang antas ng seguridad, na maihahalintulad sa pagdaragdag ng ikalawang kandado sa iyong harapang pinto.

Mga Phishing Scam

Ang phishing ay kapag sinubukan ng mga scammer na linlangin ka upang maibigay mo sa kanila ang iyong personal na impormasyon, tulad ng numero o password ng iyong credit card, sa pamamagitan ng pagpapanggap bilang isang taong pinagkakatiwalaan mo. Pangkaraniwan nila itong sinusubukan gamit ang mga pekeng email, pero puwede rin silang gumamit ng mga text message o tawag sa telepono. Palaging maging mapagmatyag!

Mga Karaniwang Palatandaan / Hudyat ng Babala ng Phishing:

- **Agarang Pananalita:** Mag-ingat sa agarang paghiling ng personal na impormasyon.
- **Di-kilalang Nagpadala:** Suriin nang mabuti ang email address ng nagpadala.
- **Kaduda-dudang Link:** Itapat ang cursor sa mga link upang makita ang aktuwal na URL bago mag-click.
- **Maling Balarila at Baybay:** Ang mga lehitimong organisasyon ay kadalasang may maayos na nakasulat na komunikasyon.
- **Di-inaasahang Attachment:** Huwag magbukas ng mga attachment na hindi mo inasahan.

Mga Tip sa Privacy ng Datos

Paano ko mababawasan ang aking digital footprint?

Ano ang digital footprint?

Tinatawag ding “digital shadow” (digital na anino) ang natatanging bakas ng datos na nagagawa ng isang tao habang gumagamit ng internet. Kasama sa footprint ng isang tao ang personal na datos na ibinabahagi niya nang tuwiran o di-tuwiran at ang impormasyon tulad ng: aktibidad sa account (mga ni-like, pakikipag-ugnayan, atbp.), kasaysayan ng pag-browse, cookies, atbp.

01 Limitahan ang mga social media account

Kapag mas kaunti ang mga account na mayroon ka, mas kaunti rin ang mailalabas mong personal na datos. I-delete ang mga luma, di-gamit, o di-aktibong account, at gawing pribado ang iyong mga aktibong account. Mababawasan mo rin ang iyong pagkalantad kung lilimitahan ang mga post sa “mga kaibigan lang” at io-off ang pagkolekta ng datos ng lokasyon.

02 I-delete ang mga lumang email address

Kung hindi mo ginagamit ang isang lumang email address, i-delete na ito. Kapag isinara mo ang mga di-gamit na email address, mababawasan ang iyong pagkalantad sa mga paglabag sa datos at ang bilang ng paraan kung paano matutunton, mananakaw, o maha-hack ang iyong impormasyon.

03 Gumawa ng email address na pang-spam

Gumawa ng account na partikular para sa mga liham-balita, promosyon, o diskuwento, at limitahan ang anumang personal na nakapagpapakilalang impormasyon (PII) na iniimbak mo sa email account na iyon. Sa ganoong paraan, mapananatili mong hindi makalat at walang spam ang iyong pangunahing inbox.

04 Kumilos nang patago

Sa tulong ng stealth (patago), o incognito mode, makakapag-surf ka ng web nang walang website at web browser tulad ng Google Chrome, Safari, at Firefox na lokal na sumusubaybay at nagse-save ng datos ng iyong aktibidad sa pag-browse.