



متن زیر به دو زبان پشتو و دری، با هدف افزایش آگاهی سایبری کارمندان و عموم مردم تهیه شده و برای انتشار در شبکه‌های اجتماعی آماده گردیده است.

د برېښنالیک امنیت | Email Security

برېښنالیک د اړیکو او کاري چارو له مهمو وسیلو څخه دی؛ خو په ورته وخت کې د سایبري مجرمینو له مهمو هدفونو څخه هم ګڼل کېږي. ډېر سایبري بریدونه له یوه جعلي یا ککر برېښنالیک څخه پیلېږي.

مهم ګواښونه:

- فیشینګ (Phishing) او جعلي برېښنالیکونه
- ککر ضمیمه فایلونه (Malicious Attachments)
- ناوړه لینکونه (Malicious Links)
- د لېږونکي د هویت جعل (Email Spoofing)
- د پسرورد او حساب معلوماتو غلا
- Ransomware او Malware

څنګه خپل برېښنالیک خوندي کړو؟

- ✓ د لېږونکي برېښنالیک پته په دقت سره وڅېړئ.
 - ✓ پر مشکوکو لینکونو کلیک مه کوئ.
 - ✓ نااشنا ضمیمه فایلونه مه پرانیږئ.
 - ✓ د پټنوم له داخلولو مخکې د وېب‌پاڼې پته په دقت سره وګورئ.
 - ✓ د خپل برېښنالیک حساب لپاره قوي او ځانګړی پټنوم وټاکئ.
 - ✓ MFA/2FA فعال کړئ.
 - ✓ خپل عملیاتي سیستم او امنیتي سافټوېرونه تازه وساتئ.
 - ✓ تر هغه چې د ترلاسه کوونکي له هویت څخه ډاډه نه یاست، حساس معلومات مه لېږئ.
- امنیتي سپارښتنه: که یو برېښنالیک په تاسو کې وېره، بېرې یا غیرعادي احساسات رامنځته کوي، نو له هر اقدام مخکې یې یو ځل بیا په دقت سره وڅېړئ.

والسلام

امنیت ایمیل | Email Security

ایمیل یکی از مهم ترین ابزارهای ارتباطی و کاری است؛ اما همزمان یکی از اهداف اصلی مجرمان سایبری نیز محسوب می‌شود. بسیاری از حملات سایبری از یک ایمیل جعلی یا آلوده آغاز می‌شوند.

مهم ترین تهدیدها:

- فیشینګ (Phishing) و ایمیل‌های جعلی
- پیوست‌های آلوده (Malicious Attachments)
- لینک‌های مخرب (Malicious Links)
- جعل هویت فرستنده (Email Spoofing)
- سرقت رمز عبور و اطلاعات حساب
- بدافزار و باج‌افزار (Ransomware)

چگونه از ایمیل خود محافظت کنیم؟

- ✓ آدرس فرستنده را با دقت بررسی کنید.
 - ✓ روی لینک‌های مشکوک کلیک نکنید.
 - ✓ پیوست‌های ناشناس را باز نکنید.
 - ✓ قبل از وارد کردن رمز عبور، آدرس وب‌سایت را بررسی کنید.
 - ✓ برای حساب ایمیل، رمز عبور قوی و منحصر به فرد انتخاب کنید.
 - ✓ MFA/2FA را فعال کنید.
 - ✓ سیستم عامل و نرم‌افزارهای امنیتی را به روز نگه دارید.
 - ✓ اطلاعات حساس را بدون اطمینان از هویت گیرنده ارسال نکنید.
- نکته امنیتی: اگر یک ایمیل باعث ایجاد ترس، عجله یا هیجان غیرعادی می‌شود، قبل از هر اقدامی آن را دوباره بررسی کنید.

والسلام

ریاست امنیت سایبری





د افغانستان اسلامي امارت

د مخابراتو او معلوماتي تکنالوجي وزارت
د تخنیکي او پالیسي معیشت
د معلوماتي تکنالوجي د زیربناوو لوی ریاست
د سایبري امنیت ریاست
د افسریت امنیت



متن زیر به دو زبان پشتو و دری، با هدف افزایش آگاهی سایبری کارمندان و عموم مردم تهیه شده و برای انتشار در شبکه‌های اجتماعی آماده گردیده است.

د عامه وای‌فای امنیت (Public Wi-Fi Security)

نن ورځ په هوتلونو، پوهنتونونو، هوايي ډگرونو او نورو عامه ځایونو کې د عامه وای‌فای کارول ډېر عام شوي دي. خو له ناپېژندل شوو شبکو سره نښلېدل کولی شي زموږ د شخصي معلوماتو او آنلاین حسابونو امنیت له خطر سره مخ کړي. برید کوونکي کېدای شي د اصلي شبکې په څېر د ورته نوم لرونکې جعلی شبکې جوړې کړي، یا په عامه شبکو کې له امنیتي کمزوریو څخه د کاروونکو معلوماتو ته د لاسرسۍ لپاره ناوړه گټه واخلي.

د دغو خطرونو د کمولو لپاره:

- ◊ له نښلولو مخکې د شبکې نوم له مسؤل کس څخه تأیید کړئ.
 - ◊ په عامه شبکو کې له حساسو فعالیتونو، لکه آنلاین بانکداری، څخه ډډه وکړئ.
 - ◊ د معلوماتو د داخلولو پر مهال ډاډ ترلاسه کړئ چې وب‌پاڼه HTTPS کاروي.
 - ◊ له Wi-Fi شبکو سره د اتوماتیک نښلېدو (Auto-Connect) وړتیا غیرفعال کړئ.
 - ◊ په موبایل او لپ‌ټاپ کې د File Sharing وړتیا غیرفعال کړئ.
 - ◊ که امکان ولری، له یوه معتبر VPN څخه استفاده وکړئ.
 - ◊ د کار له پای ته رسېدو وروسته، شبکه له خپل وسیله څخه Forget کړئ.
- یادونه: عامه وای‌فای حتمي نه ده چې ناامنه وي، خو کارول یې احتیاط او د امنیتي اصولو رعایت ته اړتیا لري. ستاسو د معلوماتو امنیت، ستاسو خپله مسؤلیت دی.

والسلام

امنیت وای‌فای عمومی (Public Wi-Fi Security)

امروزه استفاده از وای‌فای عمومی در هتل‌ها، پوهنتون‌ها، میدان‌های هوایی و سایر مکان‌های عمومی بسیار رایج است. با این حال، اتصال به شبکه‌های ناشناس میتواند امنیت اطلاعات شخصی و حساب‌های آنلاین ما را با خطر مواجه کند. مهاجمان ممکن است شبکه‌های جعلی با نام مشابه شبکه اصلی ایجاد کنند یا از ضعف امنیتی شبکه‌های عمومی برای دسترسی به اطلاعات کاربران سوءاستفاده کنند.

برای کاهش این خطرات:

- ◊ پیش از اتصال، نام شبکه را از مسئول محل تأیید کنید.
- ◊ از انجام فعالیت‌های حساس مانند بانکداری آنلاین در شبکه‌های عمومی خودداری کنید.
- ◊ هنگام ورود اطلاعات، استفاده از وب‌سایت‌های دارای HTTPS را بررسی کنید.
- ◊ قابلیت اتصال خودکار به شبکه‌های Wi-Fi را غیرفعال کنید.

◊ قابلیت File Sharing را در موبایل و لپ‌تاپ غیرفعال کنید.

◊ در صورت امکان، از یک VPN معتبر استفاده کنید.

◊ پس از پایان استفاده، شبکه را از دستگاه خود Forget کنید.

توجه: وای‌فای عمومی الزاماً ناامن نیست، اما استفاده از آن نیازمند احتیاط و رعایت اصول امنیتی است. امنیت اطلاعات شما، مسئولیت خود شماست.

ریاست امنیت سایبری

