Von zu Hause aus arbeiten - was soll ich tun?

Empfehlungen von BSI-Beratern, wie Sie und Ihr Unternehmen bei der Arbeit von zu Hause aus sicher sein können:

1. **Reisevorbereitungen - Was soll ich tun, wenn ich das Büro verlasse?**
Stellen Sie sicher, dass Sie die Kontaktdaten Ihrer IT-Abteilung haben, da Sie deren Unterstützung in den kommenden Tagen benötigen könnten. Wenn Sie gebeten werden, Ihren Laptop, Ihre Geschäfts-ausrüstung und Ihre Geschäftsdaten mitzunehmen, seien Sie vorsichtig, wenn Sie verreisen, und denken Sie an die grundlegende persönliche Sicherheit. Kriminelle sind opportunistisch, und wenn sie beispielsweise etwas hinten im Auto liegen sehen, könnte es gestohlen werden.

2. **Geschäftsinformationen - Was soll ich tun, wenn ich vertrauliche Geschäftsinformationen habe?**
Bewahren Sie es immer sicher auf und halten Sie es in Ihrem Besitz und niemals außer Sichtweite. Wenn Sie eine Pause einlegen oder die Dokumentation verlassen, verstauen Sie sie in einer sicheren Umgebung. Denken Sie daran, dass geschäftliche Informationen auch dann vertraulich bleiben müssen, wenn sie bei Ihnen zu Hause aufbewahrt werden.

3. **Verwendung von Wi-Fi zu Hause - Ich habe meinen Laptop oder mein Gerät am Arbeitsplatz noch nie an mein Wi-Fi zu Hause angeschlossen?**
Wenn Sie gebeten wurden, eine Verbindung mit dem Internet zu Hause herzustellen, stellen Sie sicher, dass Ihre Wi-Fi-Verbindung sicher und kennwortgeschützt ist, damit Sie kontrollieren können, wer sich mit ihr verbindet. Für öffentliche und ungesicherte Wi-Fi's ist der beste Ratschlag, die Verbindung mit ihnen zu vermeiden.

4. **Benutzen Sie Ihr VPN - Was ist ein VPN und wie verbinde ich mich mit ihm?** Ein VPN ist ein virtuelles privates Netzwerk, das die meisten Unternehmen verwenden, um eine sichere Verbindung zum Netzwerk über das Internet herzustellen. Die meisten Unternehmen haben eine Richtlinie für die Nutzung von VPNs und die Art und Weise, wie man sich mit ihnen verbindet - normalerweise ein kennwortgeschütztes oder Token-System. Wie Sie das herausfinden können, erfahren Sie von Ihrer IT-Abteilung als Ausgangspunkt.

5. **Phishing - Was ist Phishing und warum muss ich vorsichtig sein?**
Phishing ist eine betrügerische Praxis, bei der Betrüger oder Cyberkriminelle E-Mails versenden, die so aussehen, als seien sie seriöse und vertrauens-würdige Quellen, um Einzelpersonen dazu zu verleiten, persönliche Informationen wie Passwörter und Kreditkartennummern preiszugeben. Dies ist eine der größten Ursachen für Cyberkriminalität, und alle Benutzer sowohl am Arbeitsplatz als auch im Heimbüro müssen auf der Hut sein. Wenn Sie E-Mails sehen, die aus nicht vertrauenswürdigen Quellen stammen, melden Sie diese Ihrer IT-Abteilung und befolgen Sie deren Rat. Wenn Sie auf einen Link klicken oder einen Link herunterladen, wenden Sie sich sofort an Ihre IT-Abteilung, die über Protokolle verfügt, um das Problem zu beheben oder zu lösen.

6. **Sicherheit von Mobiltelefonen und Geräten - Ist mein Mobiltelefon sicher?**
Vielleicht auch nicht. Wir sehen eine Zunahme von Anrufen, die Sie vielleicht nicht erkennen, oder Anrufe von "unbekannten Nummern". Es ist am besten, die unbekannten Nummern nicht zu beantworten, und bei denjenigen, die von nicht erkannten Nummern aus anrufen, ist Vorsicht geboten, da bei solchen Anrufen betrügerische Aktivitäten auftreten können.

7. **Backup - Was ist ein Back-up und was muss ich tun?**
Ein Backup oder eine Datensicherung ist eine Kopie von Computerdaten, die an anderer Stelle genommen und gespeichert werden. Sie kann verwendet werden, um die Originaldaten nach einem Ereignis wiederherzustellen oder um sich auf ein mögliches Datenleck vorzubereiten. Sprechen Sie mit Ihrer IT-Abteilung darüber, was Sie sichern müssen, wie Sie es sichern können und welche Ausrüstung Sie dafür benötigen.

8. **Konferenzgespräche und interne Kommunikation - Was sind sie und warum werden sie verwendet?**
Ihr Unternehmen kann Ihnen möglicherweise über die verschiedenen Anwendungen, die Sie in Ihrem normalen Arbeitsumfeld verwenden werden, Anrufmöglichkeiten anbieten. Melden Sie sich bei Ihren Teamkollegen, die die Konferenzausrüstung Ihres Unternehmens wie WebEx, Microsoft Teams und Zoom verwenden, um nur einige zu nennen. Halten Sie sich über die Unternehmensrichtlinien und die interne Kommunikation auf dem Laufenden. Stellen Sie bei der Kundenbetreuung auch sicher, dass Ihre Kunden über diese Ausrüstung verfügen oder, falls dies nicht der Fall ist, dass sie diese Ausrüstung herunterladen und entsprechend ihrer Unternehmensrichtlinien darauf zugreifen können.

9. **Arbeitsmuster - Wie kann ich meine normalen Arbeitsgewohnheiten beibehalten?**
Behalten Sie Ihre guten Arbeitsgewohnheiten für diejenigen bei, die nicht daran gewöhnt sind, von zu Hause aus zu arbeiten, denn es kann schwierig sein, sich an die Arbeit anzupassen, und zwar für längere Zeit. Wenden Sie so viele der normalen Büroroutinen wie möglich an, wie z.B. Aufwachzeit, Anfangs- und Endzeiten, Kaffeepausen, Mittagspausen, Besprechungen und Kundeninteraktionen, auch wenn diese aus der Ferne durchgeführt werden. Je mehr in der Abfolge der normalen Büroarbeit, desto einfacher wird der Arbeitsprozess aus der Ferne.

10. **Arbeitsumgebung - Was ist für mich die beste Arbeitsumgebung?**
Schaffen Sie, wo es möglich ist, eine komfortable Arbeitsumgebung. Ergonomie ist zu Hause genauso wichtig wie im Büro. Denken Sie über die Geräte, Daten und Informationen nach, die Sie jetzt zu Hause haben werden, und wie Sie sie vor unbeabsichtigtem Anblick oder Gebrauch schützen müssen, sowie über Ihre Unternehmensrichtlinien zur Entsorgung von Daten und Informationen.

bsi.

IE/International
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us