Минимум, который работает

Мы часто повторяли, что принцип нулевого доверия — лучшая защита. Не выполнять никаких требований, пока не будет доказана их легитимность, не переходить по ссылкам, не открывать вложения, не доверять даже знакомым, пока не проверишь.

Но у этой системы есть один очевидный недостаток — ограниченность человеческих ресурсов. Наше внимание можно перегрузить, если проверять каждое сообщение, сверять адреса сайтов, перезванивать по номерам с официального сайта после каждого письма. Это неприятный факт, но абсолютно реалистичный.

И киберпреступники это прекрасно понимают. Они не взламывают системы — они взламывают внимание. Любая усталость, спешка, переключение между задачами работает на них. Поэтому важно не стремиться к идеальному «нулевому доверию», а выстроить минимальный, но устойчивый уровень защиты, который реально выдержит повседневный ритм.

Три базовых привычки:

➞Не действовать с ходу. Любая просьба «срочно», «прямо сейчас» — сигнал стоп. Даже 10 секунд паузы позволяют мозгу вернуть контроль.

➞Один канал доверия. Выберите единственный способ для критичных действий — например, только личный звонок по известному номеру. Все остальные каналы («новый чат», «альтернативный аккаунт», «резервная ссылка») автоматически под подозрением.

➞Три тревожных маркера. Срочность, эмоции, риск упустить выгоду, персональные данные. Если в сообщении есть хотя бы два — перед вами, скорее всего, фишинг или социальная инженерия.

Никакая система не даст полной гарантии. Но эти простые правила экономят главное — внимание. Именно оно остаётся последней линией обороны между человеком и злоумышленниками в сети Интернет.