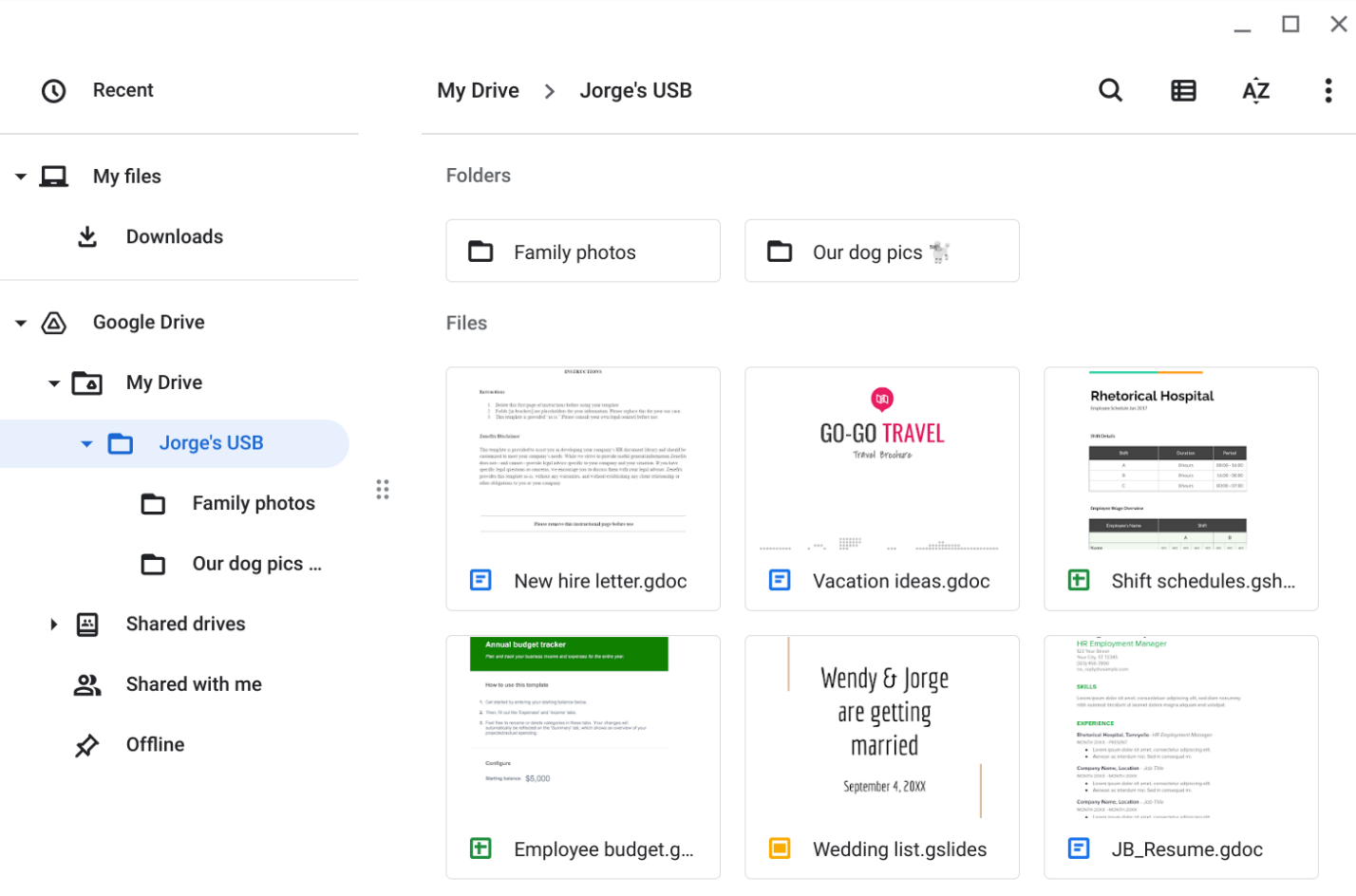
## **Exercício USB de estacionamento**

|  |  |
| --- | --- |
| **Conteúdo** | O USB contém informações pessoais identificáveis (PII), como fotos da família e do cachorro, além de documentos de trabalho sensíveis, como uma carta de nova contratação e o cronograma de turnos dos funcionários. Misturar dados pessoais com arquivos de trabalho não segue boas práticas de segurança, pois aumenta o risco de vazamento de informações e compromete a privacidade e a segurança dos dados. |
| **Mentalidade de atacante** | Essas informações podem ser usadas de várias maneiras contra Jorge e o hospital. Os cronogramas e documentos de contratação fornecem dados que um atacante pode usar para obter informações sobre a estrutura da equipe e dos horários, possibilitando um ataque de engenharia social. Um atacante pode usar essas informações para se passar por colegas de trabalho ou até familiares de Jorge, criando e-mails de phishing ou outras formas de comunicação que parecem legítimas, levando Jorge a divulgar informações confidenciais ou realizar ações prejudiciais. |
| **Análise de risco** | Para reduzir os riscos associados ao uso do dispositivo USB, é importante adotar controles técnicos, operacionais e gerenciais. Os funcionários devem ser treinados regularmente sobre os riscos de segurança de dispositivos USB e como proteger dados sensíveis. Além disso, verificações antivírus periódicas podem ajudar a detectar malware, e desabilitar o AutoPlay nos computadores evitaria a execução automática de códigos maliciosos. Isso protegeria o ambiente de trabalho contra o comprometimento e vazamento de arquivos críticos |

CENARIO: Você faz parte da equipe de segurança do Rhetorical Hospital e chega ao trabalho certa manhã. No chão do estacionamento, você encontra um USB com o logotipo do hospital impresso nele. Não há mais ninguém por perto que possa tê-lo deixado cair, então você decide pegá-lo por curiosidade.

Leva a unidade USB de volta ao seu escritório, onde a equipe tem um software de virtualização instalado em uma estação de trabalho. O software de virtualização pode ser usado exatamente para essa finalidade, pois é uma das únicas maneiras de investigar com segurança uma unidade USB desconhecida. O software funciona executando uma instância simulada do computador na mesma estação de trabalho. Essa simulação não está conectada a outros arquivos ou redes, de modo que a unidade USB não pode afetar outros sistemas se estiver infectada com software malicioso.

ARQUIVOS ENCONTRADO NO USB