A. Suppose that U and V are two gates such that $V = e^{it}U$ for some real number t. Then how do U and V act on an arbitrary state $|\psi\rangle$? Well,

$$V|\psi\rangle = e^{it}U|\psi\rangle.$$

So $V|\psi\rangle$ and $U|\psi\rangle$ are global phase changes of each other and hence the same state. So there is no practical difference between U and V as gates. Yes, there should be a caveat that U and $e^{it}U$ are actually the same gate for all real t.

B. Yes, the CNOT gate can be used in this way to clone any classical one-qbit state $|\alpha\rangle$. However, this trick does not clone general one-qbit states $|\chi\rangle$ where $\chi_0\chi_1 \neq 0$:

$$\text{CNOT} \cdot (|\chi\rangle \otimes |0\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \chi_0 \\ 0 \\ \chi_1 \\ 0 \end{bmatrix} = \begin{bmatrix} \chi_0 \\ 0 \\ 0 \\ \chi_1 \end{bmatrix} \neq \begin{bmatrix} \chi_0\chi_0 \\ \chi_0\chi_1 \\ \chi_1\chi_0 \\ \chi_1\chi_1 \end{bmatrix} = |\chi\rangle \otimes |\chi\rangle.$$

So this trick is not a way around the no-cloning theorem. Cloning classical states is easy — classical computers do it all the time — but cloning non-classical states still seems impossible.

C. By re-doing our analysis from class [which I'll omit here], we see that the measurement produces $|0\rangle \otimes |1\rangle$ if f is constant or $|1\rangle \otimes |1\rangle$ if f is not constant. Therefore the algorithm still solves Deutsch's problem, albeit with the decision at the end reversed from how we studied it.

D. To solve the problem, we can draw a tree with branches for $|\alpha\rangle = |0\rangle$ vs. $|\alpha\rangle = |1\rangle$, for $U = I$ vs. $U = H$, etc. [which I'll omit here]. There are 18 leaves producing these probabilities:

- Prob(success declared with $|\alpha\rangle = |\beta\rangle$) = 3/8.
- Prob(success declared with $|\alpha\rangle \neq |\beta\rangle$) = 1/8.
- Prob(failure declared with $|\alpha\rangle = |\beta\rangle$) = 1/4.
- Prob(failure declared with $|\alpha\rangle \neq |\beta\rangle$) = 1/4.

The overall success rate is 1/2, which is what it would be without eavesdropping. So Ariko and Babatope cannot detect eavesdropping through the success rate alone. However, they can detect eavesdropping by generating twice as many random bit values as needed and comparing half of them. When they do this, about 1/4 of their supposed successes are revealed to be failures. [By the way, this cryptosystem is due to Bennett and Brassard (1984).]