Sicurezza Informatica applicata allo Studio professionale

Relatore: Davide Peruzzi

OPEN Dot Com

OPEN Dot Com

Password

- Minimo 8 caratteri
- Maiuscole e minuscole
- Numeri e caratteri speciali
- Cambiata ogni 3 mesi

Queste sono solo le minime misure. Potete migliorare:

- Un paio di caratteri in più non guastano
- Non usare parole di senso compiuto
- Non condividetele

Usate password diverse tra questi ambiti (almeno)

Accesso al WEB | WiFi | Accesso al PC | Account email

OPEN Dot Com

Comunicazioni sicure con HTTPS

- Le comunicazioni HTTP inviano il traffico «in chiaro» e possono essere intercettate e lette
- Le comunicazioni importanti devono avvenire in HTTPS che è più sicuro

Come faccio a verificare se mi sto collegando ad un sito in HTTPS?

Quando dobbiamo assolutamente verificare che le trasmissioni siano in HTTPS?

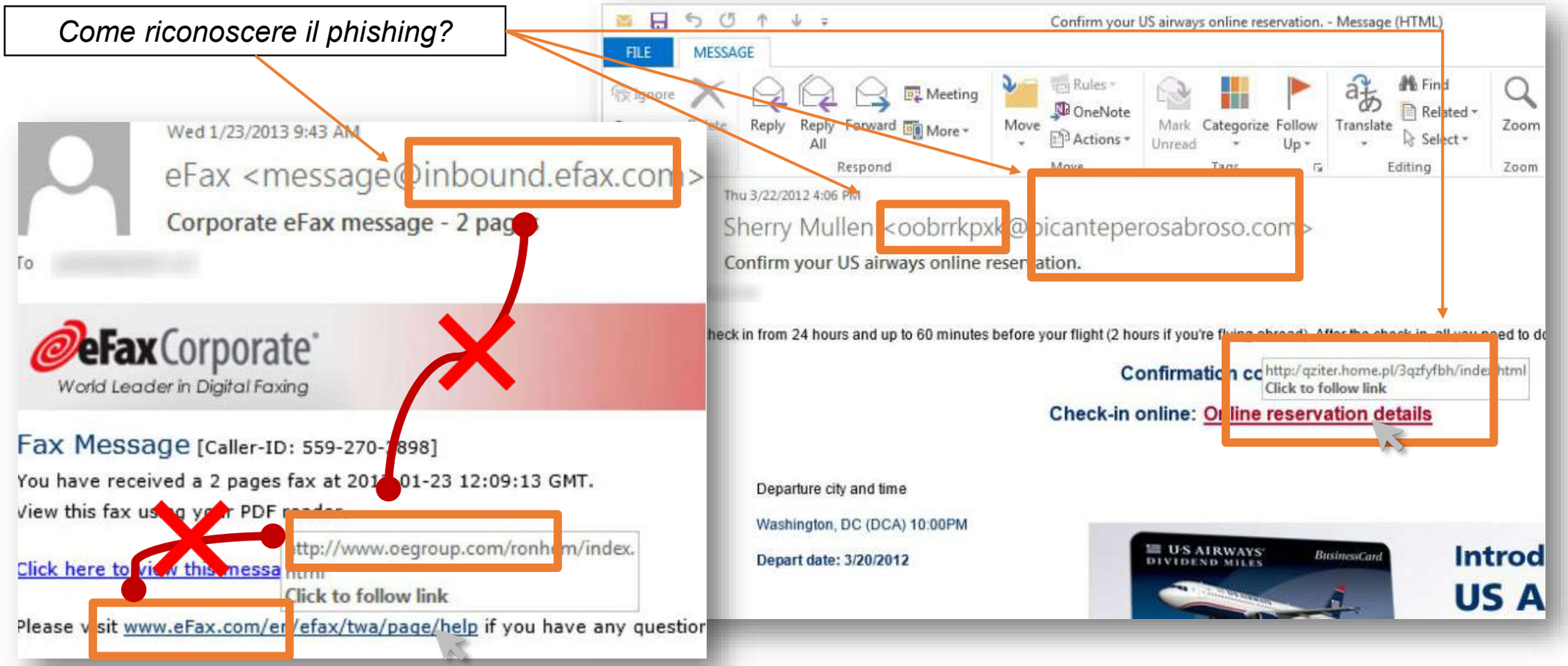
Tutte le volte che inseriamo un dato sensibile su un sito web come password, codici bancari, dati di clienti o personali

OPEN Dot Com

PEC e phishing

Le email ricevute sulla PEC non sono assolutamente più sicure rispetto a quelle ordinarie!

Come riconoscere il phishing?



Il decalogo per combattere il phishing

1. Le caselle **PEC non sono sinonimo di sicurezza**: ultimamente sono le più utilizzate per fini malevoli.
2. Un **mittente conosciuto non è** costituisce una **garanzia**.
3. Non è raro ricevere mail dal **contenuto malevolo in risposta ad una mail** da voi inviata.
4. **Diffidate di mail che** hanno un testo molto conciso e/o che **palesano urgenza nell'apertura dell'allegato** (es. "prego visionare rapidamente l'allegato" o "fattura in scadenza").
5. Il linguaggio utilizzato nelle mail malevole è migliorato notevolmente: **vanno analizzati attentamente anche i particolari** (es. firma, contesto, forma, etc.).
6. **Prestare estrema attenzione ai link contenuti nella mail**, anche a quelli presenti in eventuali allegati.
7. **Mai aprire un allegato protetto da password**: è sicuramente un malware!
8. **Il formato documentale standard per documenti di carattere lavorativo è il PDF**: diffidate di tutti gli allegati word, excel e zip. Apriteli solo se siete assolutamente certi che non contengano malware.
9. **Ricordatevi che ogni comunicazione ufficiale**, giudiziaria, multe o simili **non vi arriverà mai via email**, ma tramite raccomandata! (al limite **su una PEC da un'altra PEC**)
10. La regola più importante di tutte: **usate il buonsenso!** Non cliccate furiosamente su tutte le mail che ricevete.

OPEN Dot Com

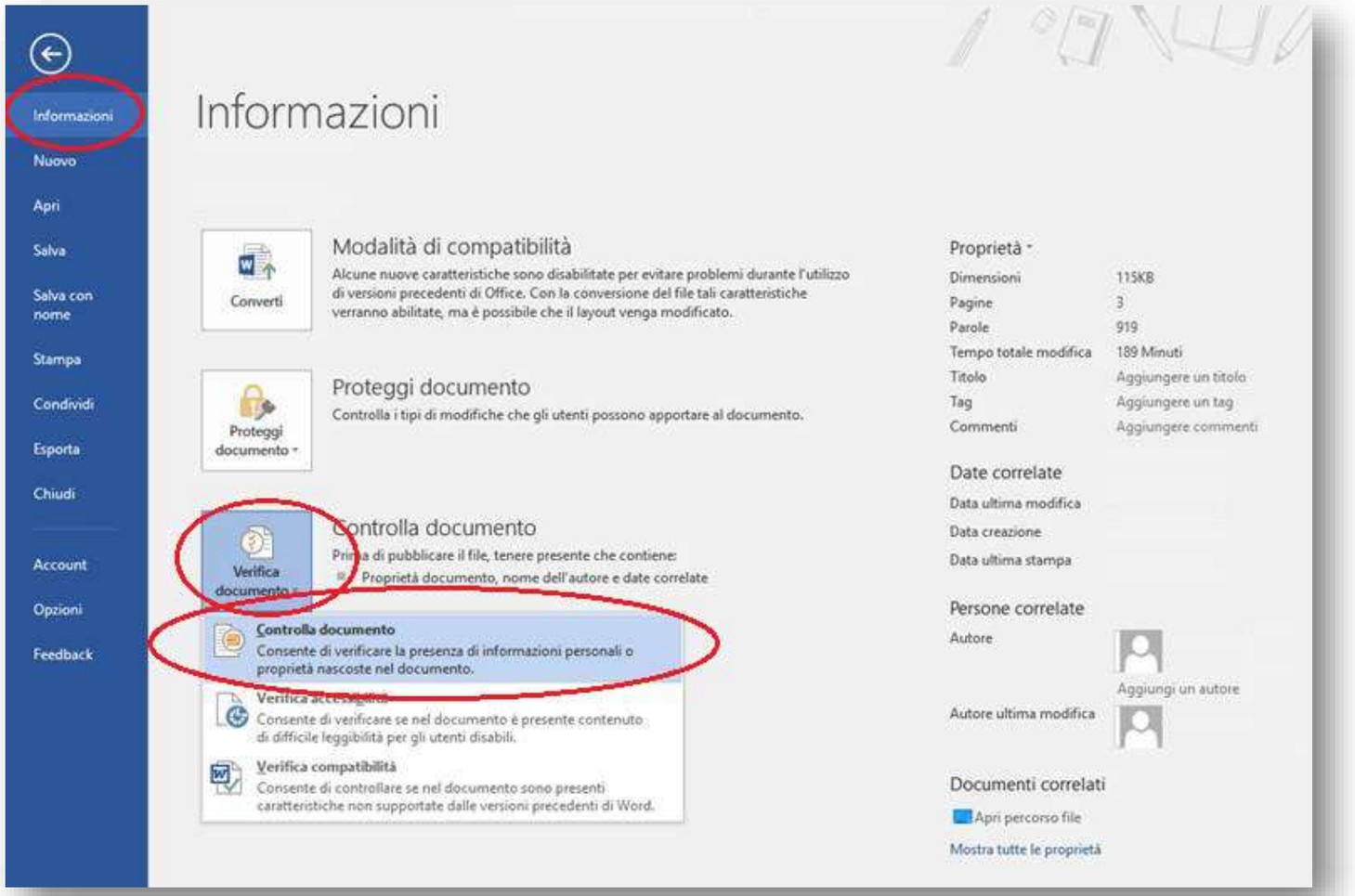
Divulgazione inconsapevole di dati

Ricordatevi che prima di rendere pubblico un documento è buona norma verificare che non contenga dati personali

In tutti i programmi della suite Office, è possibile rimuovere automaticamente tutte le informazioni personali (FILE > Informazioni > Verifica Documento > Controlla Documento)

Un'altra operazione utile è cancellare i metadati dei file da pubblicare.

I metadati sono visualizzabili con un semplice click del tasto destro sul file e poi selezionando Proprietà. Dalla scheda Dettagli è possibile non solo avere una panoramica di tutti i metadati contenuti nel file, ma anche rimuoverli grazie alla voce Rimuovi proprietà e informazioni personali.



Attenti agli insider

La maggior parte degli attacchi informatici parte da un utente interno alla struttura detto «insider».
Normalmente sono persone scontente oppure pagate per danneggiarvi.

Il modo migliore di combatterli è avere strumenti di log certi e renderlo noto a dipendenti e collaboratori.

Il Log degli Amministratori

- È fortemente consigliato e in molti ambiti obbligatorio
- Ha un basso impatto economico
- Ha una bassa manutenzione
- È un ottimo deterrente per combattere gli attacchi di insider
- È un metodo sottovalutato per aumentare la sicurezza informatica

GRAZIE PER L'ATTENZIONE

Per informazioni: info@opendotcom.it

Sito: www.opendotcom.it

OPEN Dot Com