Sharing good Practices for European mobility Activities Development

SPREAD
Sharing good Practices foR European mobility Activities Development

Erasmus+ KA2 – Strategic Partnerships

Project number: 2016-1-IT01-KA202-005504

Computer safety and protection of data – basic concepts

LTTA-4: 16th October – 20th October 2017
Rzeszów, Poland

DANMAR COMPUTERS
IT matters

Topics covered

SPREAD
Sharing good Practices foR European mobility Activities Development

COMPUTER SAFETY AND PROTECTION OF DATA

- Virtual Private Networks, basics of SSL protocol security of providing sensitive information over various channels and networks
- Email security: viruses and malware, using digital signatures and message encryption

Introduction

SPREAD
Sharing good Practices foR European mobility Activities Development

Computer safety and security can be complex and intimidating, but when it comes to security in SMEs and homes, several simple steps can minimize the risks.

As a general rule: no system, network or device can be considered 100% secure.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

SPREAD
Sharing good Practices foR European mobility Activities Development

Don’t use outdated devices, operating systems and applications

Why:

„In **computer security**, a **vulnerability** is a weakness which allows an attacker to reduce a system's information assurance. **Vulnerability** is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.” [Wikipedia]

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Enable Automatic Updates

- All the software we use every day is likely riddled with security issues. These security issues are constantly being found—whether we're talking about Windows, Internet Explorer, Mozilla Firefox, Google Chrome, the Adobe Flash plugin, Adobe's PDF Reader, Microsoft Office—the list goes on and on.
- These days, a lot of operating systems and programs come with automatic updates to close these security holes. No longer do you need to click a button or download a file to update your software; it'll update itself in the background without any input from you.
- Some people like to turn this off for one reason or another. Maybe you don't like that Windows restarts after installing an update, or maybe you just don't like change. But from a security perspective, you should always leave automatic updates on.

SPREAD
Sharing good Practices foR European mobility Activities Development

Erasmus+
Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

What is a computer virus?

„ A **computer virus** is a program, script, or macro designed to cause damage, steal personal information, modify data, send e-mail, display messages, or some combination of these actions.” [Wikipedia]

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

What is malware?

„Malware is **mal**icious soft**ware** designed to change your settings, delete software, cause errors, watch browsing habits, or open computer to attacks”

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

What is malware - types

- Worm is a type of malware that can self-replicate without a host program; worms typically spread without any human interaction or directives from the malware authors.
- Trojan horse is a malicious program that is designed to appear as a legitimate program; once activated following installation, Trojans can execute their malicious functions.
- Spyware is a kind of malware that is designed to collect information and data on users and observe their activity without users' knowledge.

SPREAD
Sharing good Practices foR European mobility Activities Development

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

What is malware - types

- Ransomware, for example, is designed to infect a user's system and encrypt the data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
- Rootkit is a type of malware designed to obtain administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
- A backdoor virus or remote access Trojan (RAT) is a malicious program that secretly creates a backdoor into an infected system that allows threat actors to remote access it without alerting the user or the system's security programs.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

How do avoid and detect

- Read the messages which your computer is displaying!
- Use common sense. Advert saying „You just won the prize!” should sound suspicious.
- Do not download anything which might be even remotely suspicious
- Be aware of phishing emails and attachements

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

Tax Invoice

APPLE ID
k.ciapala@danmar-computers.com.pl

DATE
14 August, 2017

ORDER ID
MQHWYGWKHY

DOCUMENT NO.
144171387078

BILLED TO
Moonton Inc.

TOTAL
$49.99

App Store	TYPE	PURCHASED FROM	PRICE
Mobile Legends: Bang bang, 2,500 Diamonds Report a Problem	In-App Purchase	App Store	$49.99
		TOTAL	$49.99

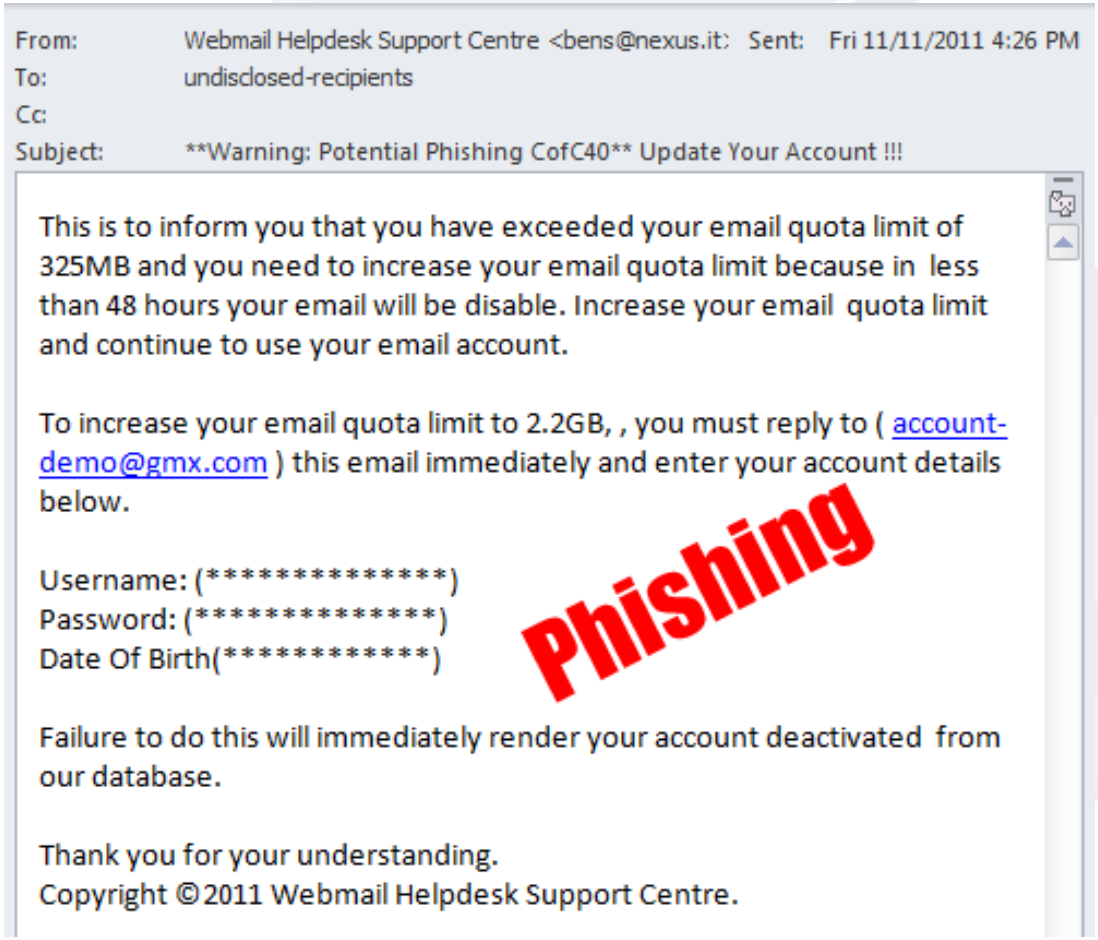
Issues with this transaction?
If you haven't authorized this transaction ,click the link below to get full refund:
Customer Support

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware



From: Webmail Helpdesk Support Centre <bens@nexus.it> Sent: Fri 11/11/2011 4:26 PM
To: undisclosed-recipients
Cc:
Subject: **Warning: Potential Phishing CofC40** Update Your Account !!!

This is to inform you that you have exceeded your email quota limit of 325MB and you need to increase your email quota limit because in less than 48 hours your email will be disable. Increase your email quota limit and continue to use your email account.

To increase your email quota limit to 2.2GB, , you must reply to (account-demo@gmx.com) this email immediately and enter your account details below.

Username: (**********)
Password: (**********)
Date Of Birth(**********)

Phishing

Failure to do this will immediately render your account deactivated from our database.

Thank you for your understanding.
Copyright ©2011 Webmail Helpdesk Support Centre.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

From: "Bank"<payment@epayment.com>
Subject: **Re: new payment on your account**
Date: March 24, 2014 10:39:01 AM MDT
Reply-To: <bankwiretransferdepartment@gmail.com>

Please find attached bank slip for new payment on your account.

Regards,

Account Department.

new payment.zip

SPREAD
Sharing good Practices foR European mobility Activities Development

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Antivirus and anti-malware

Last line of defence:

- Use antivirus software, from company which has good reputation
- In case of suspicious behaviour, use on demand scanners, like Malwarebytes Anti-malware
- Use trusted email providers
- Be careful with online file sharing services

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

Let's talk passwords

- Do not use the same password for important data and not-so-important data
- Complex 8-characters long password takes less than 10 hours to break
- NEVER ever use easy passwords below 10 characters
- Recommended: use complex passwords with password manager
- Whenever possible, use device authenticators, e.g. Google Authenticator

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

The basics

A tale about the backup

It is said that there are two types of computer users

- Those who make backup
- Those who will

SPREAD
Sharing good Practices foR European mobility Activities Development

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Introduction to encryption

SPREAD
Sharing good Practices foR European mobility Activities Development

- Fundamentally, encryption is the act of scrambling communication to stop people other than its intended recipient from reading it.
- In various forms, the technique dates back millennia - Julius Caesar used basic encryption in messages to his generals
- Modern encryption is complex, but with correct implementation - very secure

Introduction to encryption

SPREAD
Sharing good Practices foR European mobility Activities Development

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Introduction to encryption

SPREAD
Sharing good Practices foR European mobility Activities Development

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Introduction to encryption

A digital certificate is an electronic "passport" that allows a person, computer or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate may also be referred to as a public key certificate.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Introduction to encryption

Digital certificate can provide:

Identification / Authentication:

The persons / entities with whom we are communicating are really who they say they are.

Confidentiality:

The information within the message or transaction is kept confidential. It may only be read and understood by the intended sender and receiver.

Integrity:

The information within the message or transaction is not tampered accidentally or deliberately with en route without all parties involved being aware of the tampering.

Non-Repudiation:

The sender cannot deny sending the message or transaction, and the receiver cannot deny receiving it.

Access Control:

Access to the protected information is only realized by the intended person or entity.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Introduction to encryption

Where Digital certificates and encryption are used?

Secure HTTP = HTTPS

Email encryption

Email signatures

End to end encryption

Disks, files, mobile devices, VPNs, data transmission, email transmission, voice transmission…

*** EVERYWHERE***

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

Browsing web securely – HTTPS

Hyper Text Transfer Protocol Secure (**HTTPS**) is the secure version of **HTTP**, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of **HTTPS** stands for 'Secure'. It means all communications between your browser and the website are encrypted.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

Browsing web securely – HTTPS

How it works:

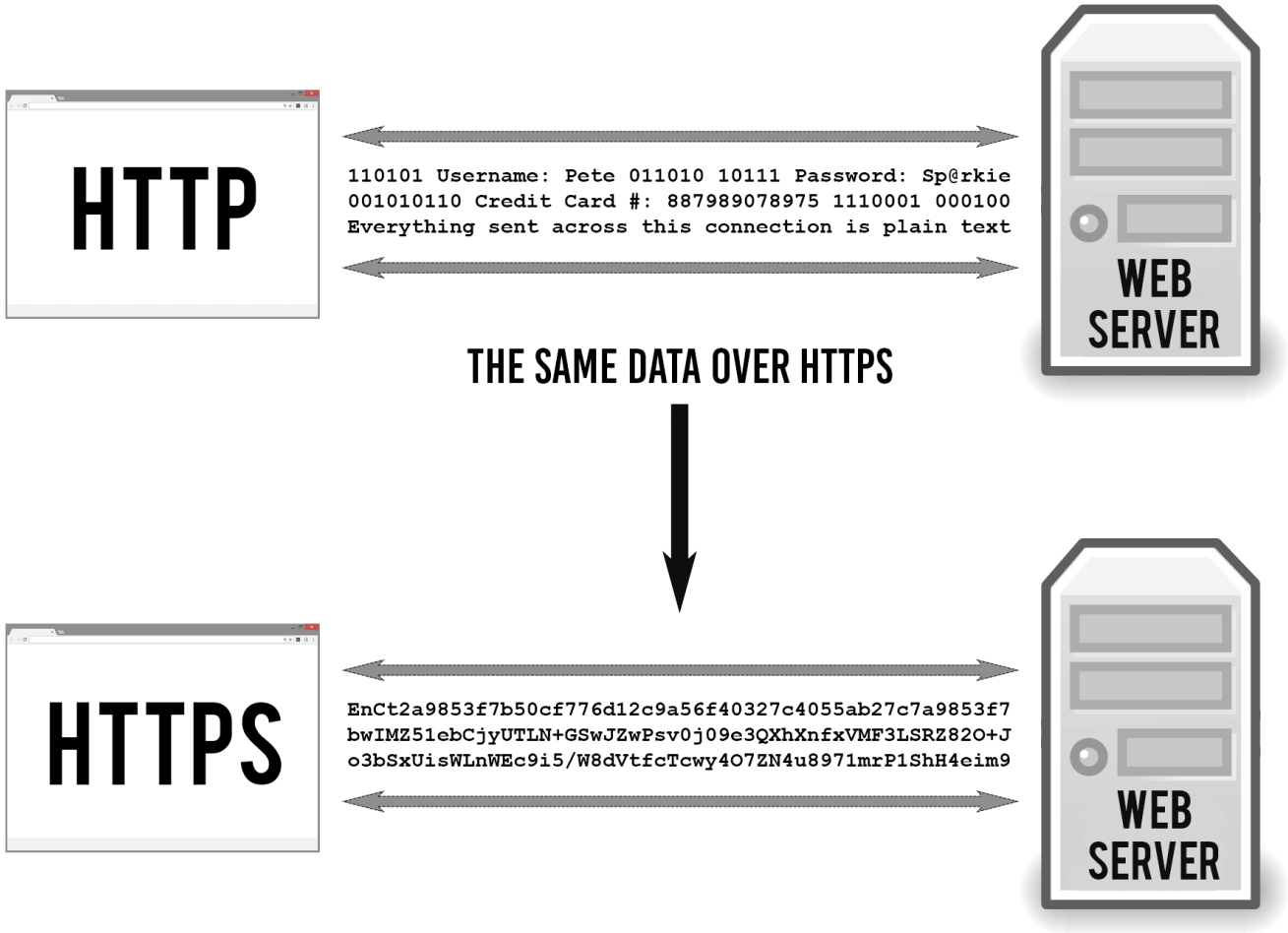
- Your browser asks for https session
- Server sends his public key
- Browser generates symmetric key and encrypts it with server's public key, then sends it back to the server
- Server decrypts session key with his private key
- Symmetric connection takes over

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

Browsing web securely – HTTPS



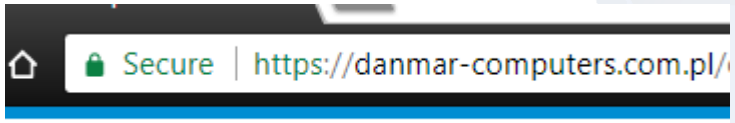
Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

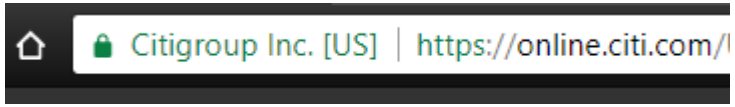
Browsing web securely – HTTPS

Standard HTTP protocol – not secure



HTTPS protocol – secure, domain validation

HTTPS protocol – secure, extended validation



HTTPS protocol – secure, extended validation

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

Secure transmission of emails – SMTP TLS

- Computer A connects to Computer B (no security)
- Computer B says “Hello” (no security)
- Computer A says “Lets talk securely over TLS” (no security)
- Computer A and B agree on how to do this (secure)
- The rest of the conversation is encrypted (secure)

Not all systems supports this method – and there is no easy way to tell if they do.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Wireless encryption

WEP – retired, very weak protection, can be cracked in minutes

WPA – retired, 128-bit version is vulnerable

WPA2 personal – current standard, fairly secure if long key is used. Enabling WPS (Wi-Fi Protected Setup) weakens security significantly.

WPA2 Enterprise – not feasible for home use.

WPA2 Personal + WPS could be cracked below 10 hrs.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Wireless encryption

Security ranking:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP is there as a fall-back method)
4. WPA + TKIP
5. WEP
6. Open Network (no security at all)

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

Signing and encrypting emails S/MIME

- First, you need S/MIME certificate, e.g. comodo.com (basic version, for personal use)
- Signing the email allows content and sender verification – nothing more
- Pretty much all email systems will support reading, but not all signing, e.g. most web-based email providers doesn't offer this functionality

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Encryption - examples

Signing and encrypting emails S/MIME

- Encrypting email is more complex
- Despite many standards being in use, not everything is compatible
- It’s not that easy to setup
- **You have to have your recipient public key – otherwise it will not work at all**

Encryption - examples

Signing and encrypting emails S/MIME

Obvious advantage – the message can’t be read by anyone apart from intended recipient

Not very popular – due to complex setup and requirements

VPN basics

VPN stands for Virtual Private Networking

- **Remote-Access**—Also called a Virtual Private Dial-up Network (VPDN), this is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations.
- **Site-to-Site**—Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. A site-to-site VPN built between offices of the same company is said to be an intranet VPN, while a VPN built to connect the company to its partner or customer is referred to as an extranet VPN.

SPREAD
Sharing good Practices foR European mobility Activities Development

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

VPN basics

VPN stands for Virtual Private Networking

Public VPN providers – fairly recent approach, allows to hide your real IP and geolocation, as well as improve anonymity and add another layer of security.

Good providers are usually paid

Not all ISPs allow VPN connections

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504

Wake up everybody!!

A question or two would be nice.

Erasmus+

Project Number: 2016-1-IT01-KA202 -005504