Hacker Wars – Knowledge Is Your Best Defense

Information Security by the Numbers

- $181 billion lost to banking fraud in 2016
- $81.6 billion spent in 2015 by organizations worldwide on information security (5.9% from 2013)
- $7.35 million sets a new high in 2017 for average cost of a data breach

Growing Sophistication and Risk

- 60% of global fraudrong organizations from mobile devices

Various Networks and Approaches

- Deep Web
- Dark Web
- Ransomware
- Malware
- DDOS

Increasingly Challenging Future

- 52% rising trend in mobile device incidents
- 24% rising trend in mobile device incidents
- 24% rising trend in mobile device incidents

Here's How to Fight Back

1. Always keep systems patched & antivirus updated.
2. Take advantage of automatic software updates.
3. Never download email attachments from unknown senders.
4. If you must open an attachment, scan it for viruses first.
6. Type the website address into your browser or search engine.
7. Suspicious? Contact your security team immediately.
8. Don’t wait – sometimes every minute counts.
9. Member and staff education. Topics include password management and credit monitoring.

Data Breaches 2017

- Malicious or Criminal: 24%
- Employee Negligence: 24%
- System Glitches: 52%

Sources: Frank Onfraud.com, Gartner, Inc., Ponemon Institute, RSA Security LLC, Symantec

Fraudulent Emails Seeking Personal Information

Lost to Banking Fraud in 2016

Money Transfer

Ransomware

Phishing

Stop.Don’t.Open.

Suspicious?

Contact your security team immediately.

Never click links in suspicious-looking emails.

Type the website address into your browser or search engine.

Suspicious?

Contact your security team immediately.

Never click links in suspicious-looking emails.

Take advantage of automatic software updates.

Never download email attachments from unknown senders.

If you must open an attachment, scan it for viruses first.

Never download email attachments from unknown senders.

If you must open an attachment, scan it for viruses first.

Member and staff education. Topics include password management and credit monitoring.

Fraudulent Emails Seeking Personal Information

Lost to Banking Fraud in 2016

Money Transfer

Ransomware

Phishing

Stop.Don’t.Open.

Suspicious?

Contact your security team immediately.

Never click links in suspicious-looking emails.

Type the website address into your browser or search engine.

Suspicious?

Contact your security team immediately.

Never click links in suspicious-looking emails.

Take advantage of automatic software updates.

Never download email attachments from unknown senders.

If you must open an attachment, scan it for viruses first.

Never download email attachments from unknown senders.

If you must open an attachment, scan it for viruses first.

Member and staff education. Topics include password management and credit monitoring.